레거시 의료기기의 사이버보안을 위한 원칙 및 실무

(Principles and Practices for the Cybersecurity of Legacy Medical Devices)

2023. 11.

식품의약품안전처
의 료 기 기 안 전 국

본 문서의 원문(Principles and Practices for the Cybersecurity of Legacy Medical Devices)은 전 세계 의료기기 규제당국자들이 자발적으로 구성한 국제의료기기규제당국자포럼(IMDRF)에서 이해당사자 간 협의를 통해 개발되었습니다.

본 문서는 IMDRF에서 발행한 원문을 식품의약품안전처가 알기 쉽게 기술한 것입니다.

본 문서는 대외적으로 법적 효력을 가지는 것이 아니므로 본문의 기술방식('~하여야 한다' 등)에도 불구하고 민원인 여러분께서 준수하셔야 하는 사항이 아님을 알려드립니다. 또한, 본 문서는 2023년 11월 현재 과학적·기술적 사실 등을 토대로 작성되었으므로 이후 구체적인 사실관계 등에 따라 달리 적용될 수 있음을 알려드립니다.

※ 본 문서에 대한 의견이나 문의 사항이 있으면 의료기기안전국 의료기기정책과에 문의하시기 바랍니다.

전화번호: 043-719-3766

팩스번호: 043-719-3750

목 차

1.0 소개

의료기기 사이버보안을 위한 원칙 및 실무(이하 IMDRF N60 지침: IMDRF/CYBER WG/N60 FINAL:2020)는 의료기기의 제품 수명 전주기(이하 TPLC: Total Product Life Cycle)에 걸친 기본 보안 원칙과 모범 실무를 제시하고 있다. 이 지침이 전 세계적으로 채택되기 위한 전제 조건은 이 지침에 포함된 권장 사항을 성공적이고 일관되게 이행하는 것이다. 이러한 이행을 위해서는 지침의 특정 과제에 집중적으로 관심을 기울이는 것이 중요하며, 이는 TPLC 전반에 걸친 의료기기 사이버 보안의 복원력을 더욱 발전시키기 위한 자연스러운 진행 과정이다.

현대 의료기기 설계는 사이버보안 고려 사항 개선의 이점을 얻지만, 현재 사용 중인 많은 의료기기는 제조업체(이하 MDM: Medical Device Manufacturers)이 의도한 의료기기 수명을 초과하는 경우를 포함하여 동일한 고려 사항이 적용되지 않는다. 이러한 의료기기들은 현재의 모범 실무에서 권장하는 것처럼(예: 패치 또는 기타 업데이트 등을 통해) 사이버보안 위협을 충분히 완화할 수 없고, 환자에게 위험을 초래할 수 있다. 또한, 보안 통제 기능이 불충분하거나 전혀 없을 수도 있고, 배치 당시에는 최첨단 보안 통제 기능이 포함되어 있었으나 헬스케어 기술의 긴 수명으로 인해 이제는 방어할 수 없는 예기치 않은 위협에 직면할 수도 있다. 이러한 의료기기들은 종종 '레거시(Legacy) 의료기기'라고 불리며, TPLC 전반에 걸친 사이버보안을 유지하기 위해 종종 다른 수단이 필요하다. 하지만 의료기기의 수명이

레거시 의료기기 여부를 결정하는 유일한 요소는 아니라는 점에 유의해야 한다. 즉 비교적 최신 의료기기지만, 최신 사이버보안 위협에 대해 합리적으로 보호할 수 없으면 연식과 관계 없이 사이버보안의 맥락에서 레거시로 간주된다. TPLC 계획을 적절히 실행할 수 있는 직원과 자원이 부족한 조직에서는 이러한 레거시 의료기기 및 관련 위험이 무기한 지속될 수 있다.

레거시 의료기기는 오늘날에도 여전히 의료 서비스를 제공하는 데 사용되기 때문에 환자 안전에 심각한 위협이 될 수 있다. 이러한 맥락에서 본 지침 문서의 목적은 MDM 및 HCP와 같은 이해관계자에게 제공되는 세부 권장 사항을 포함하여 IMDRF N60 지침에 명시된 레거시 의료기기 개념적 프레임워크를 운영하기 위한 것이다. 이 지침의 목적상 HCP에는 의료 서비스 제공 기관이 포함된다.

본 지침 문서의 목적은 이해관계자에게 잠재적인 레거시 의료기기를 식별하는 명확한 방법과 레거시 의료기기의 사이버보안을 유지하기 위한 실용적이고 실현 가능한 접근 방식을 제공하는 것이다. 본 문서는 이해관계자에게 각 관할권의 규제 시스템을 왜곡하지 않으면서 구현할 수 있는 다양한 선택지를 제공하기 위한 것으로, 이 작업은 IMDRF N60 지침을 보완하기 위한 것이다.

레거시 사이버보안 위험 관리와 관련된 추가 권장 사항은 미국 보건 부문 조정 위원회(HSCC: US Health Sector Coordinating Council)의

보건 산업 사이버보안 - 레거시 기술 보안 관리(HIC-MaLTS: Health Industry Cybersecurity - Managing Legacy Technology Security)를 참조하면 된다.

2.0 범위

이 문서는 기존 의료기기에 TPLC를 적용하는 방법에 관한 구체적인 권장 사항을 제공하여 이전 IMDRF N60 지침에서 제시된 프레임워크의 이행을 지원하기 위해 작성되었다. 이 문서는 IMDRF N60 지침을 보완하는 것으로, 관련 의료기기(체외 진단(IVD: In Vitro Diagnostic) 의료기기 포함)의 범위와 환자에게 해를 끼칠 가능성에 대해 초점을 맞춘다는 것은 변함이 없다.

이 지침은 소프트웨어(펌웨어 및 프로그램 가능 논리 제어기(이하 PLC: Programmable Logic Controller)를 포함)를 내장한 레거시 의료기기(예: 페이스메이커, 인퓨전 펌프 등)나 레거시 소프트웨어 의료기기(이하 SaMD: Software as a Medical Device)에 대한 사이버보안을 고려한다. 대부분의 규제기관이 의료기기의 안전성 및 성능에 대한 권한을 가지고 있으므로, 이 지침의 범위는 환자에게 해를 끼칠 가능성에 대한 고려 사항에 한정된다는 점에 유의해야 한다. 예를 들어, 성능에 영향을 미치거나 임상적 운영에 부정적인 영향을 미치거나 오진단 또는 잘못된 치료를 야기하는 사이버보안 위험이 본 문서의 범위에 해당한다. 개인정보(데이터) 보호 침해와 관련된 문제와 같은 다른 유형의 피해도 중요하지만, 본 문서에서는 다루지 않는다.

레거시 의료기기는 이전에 IMDRF N60 지침에서 현재의 사이버보안

위협으로부터 합리적으로 보호할 수 없는 의료기기로 정의되었다. 따라서 이 문서는 사이버보안의 맥락에서만 레거시 의료기기를 다루며, 의료기기가 '레거시'로 간주될 수 있는 다른 모든 상황(예: 의료기기의 구형 모델)에 대해서는 다루지 않는다.

위의 레거시 정의에 따라 현재 사용 중인 많은 의료기기가 레거시 의료기기로 간주될 수 있다. 이러한 현재 상태에서 보다 이상적인 미래 상태로 전환하기 위해 IMDRF N60 지침에서는 레거시 의료기기를 위한 TPLC 프레임워크를 제안했으며, 이 문서에서 더 자세하게 설명한다. 이 프레임워크의 주요 특징은 MDM과 HCP 간의 효과적인 의사소통을 통해 적시에 계획적으로 의료기기를 도입하고 폐기하여 사용 중인 레거시 의료기기의 수를 최소화하는 것이다. 이 지침의 범위를 벗어나지만, MDM과 HCP는 관련성이 있는 경우 환자에게 수명 주기 단계 정보를 전달해야 한다. 리셀러들(예: 리라벨러들(Re-labellers))은 MDM과 같은 규제 의무가 없는 경우가 많으므로 이 지침의 범위에서 제외된다.

특히 이 문서의 목적은 다음과 같다:

- 각 단계에서 명확하게 정의된 MDM 및 HCP의 책임과 함께 TPLC 프레임워크(개발, 지원, 제한적 지원 및 지원 종료)의 맥락에서 레거시 의료기기 사이버보안에 대한 설명
- MDM과 HCP에게 의사소통(취약점 관리 포함), 위험관리, HCP로의

책임이전에 대한 권장 사항을 제공.

- 지원 종료 후 보완된 통제(Compensating Controls)와 관련된 권장 사항을 제공
- 의료기기 사이버보안을 위한 TPLC 프레임워크 이전에 개발되어 여전히 사용되고 있는 기존 레거시 의료기기를 다루는 것에 대한 MDM 및 HCP의 실행 고려 사항을 제공

이전 IMDRF N60 지침에서 강조한 바와 같이, 이 문서는 사이버보안이 MDM 및 유통업체, HCP, 사용자, 규제기관, 소프트웨어 벤더를 포함하되 이에 국한되지 않는 모든 이해관계자의 공동책임임을 지속적으로 인식하고 있다.

의료기기의 유형 및 규제의 차이로 인해 추가적인 고려 사항이 필요한 특정 상황이 발생할 수 있다는 점에 유의해야 한다.

3.0 정의

본 문서의 목적을 위해, IMDRF/GRRP WG/N47 FINAL:2018 및 IMDRF/CYBER WG/N60 FINAL:2020에 명시된 용어와 정의가 적용되며, 다음의 용어 및 정의도 적용된다.

3.1 **애플리케이션 소프트웨어(Application software)**: 1. 컴퓨터 자체를 제어하는 소프트웨어와는 구별되는, 사용자가 특정 작업을 수행하거나 특정 유형의 문제를 처리할 수 있도록 설계된 소프트웨어 2. 애플리케이션 문제 해결에 특화된 소프트웨어 또는 프로그램(ISO/IEC 2382:2015)

3.2 **자산(Asset)**: 개인, 조직 또는 정부에 가치가 있는 물리적 또는 디지털 개체(ISO/IEC JTC 1/SC 41 N0317, 2017-11-12)

3.3 **가용성(Availability)**: 인가된 개체가 필요에 따라 접근가능하고 사용가능한 속성(ISO/IEC 27000:2018)

3.4 **보상적 위험 통제 조치(동의어: 보상 통제)(Compensating Risk Control Measure, syn. Compensating Control)**: 기기 설계의 일부로 구현된 위험 통제 조치 대신(또는 없이) 배치되는 특정 유형의 위험 통제 조치(AAMI TIR97:2019)

참고: 보상적 위험 통제 조치는 영구적이거나 일시적일 수 있다(예: MDM이 추가적인 위험 통제 조치를 포함하는 업데이트를 제공할 수 있을 때까지)

3.5 **컴포넌트(Component)**: (a) 시스템의 물리적 또는 논리적 부분을 형성하고, (b) 특정한 기능과 인터페이스를 가지며, (c) 시스템의 다른 부분과 독립적으로 존재하는 것으로 취급되는(예: 정책 또는 사양) 시스템 자원의 모음(ISO 81001-1:2021)

참고: 의료기기에서 컴포넌트에는 완제품, 포장 및 라벨이 부착된 의료기기의 일부로 포함되도록 의도된 모든 원자재, 물질, 조각, 부품, 소프트웨어, 펌웨어, 라벨링 또는 조립품이 포함된다.

3.6 **기밀성(Confidentiality)**: 권한이 없는 개인, 개체 또는 절차에 정보를 제공하거나 공개하지 않는 속성(ISO/IEC 27000:2018)

3.7. **구성(Configuration)**: 정보 처리 시스템의 하드웨어와 소프트웨어가 구성되고 상호 연결되는 방식(ISO/IEC 2382:2015)

3.8 **구성 관리(Configuration management)**: 구성을 지시하고 통제하기 위한 조정된 활동(ISO/IEC TR 18018:2010)

3.9 **조정된 취약점 공개(CVD: Coordinated Vulnerability Disclosure)**: 연구자 및 기타 이해관계자가 제조업체와 협력하여 취약점 공개 및 관련 위험을 줄이는데 필요한 해법을 찾는 절차(AAMI TIR97:2019)

참고: 이 절차에는 취약점 및 해결 방법에 대한 정보를 보고, 조정 및 출판하는 등의 작업이 포함된다.

3.10 **사이버보안(Cybersecurity)**: 정보와 시스템이 무단 접근, 사용, 유출, 중단, 수정 또는 파괴와 같은 비인가 활동으로부터 보호되어 기밀성, 무결성, 가용성과 관련된 위험을 수명 주기 전체 동안 수용할 수 있는 수준으로 유지되는 상태(ISO 81001-1:2021)

3.11 **폐기(Decommission)**: 활성 서비스에서 제거(ASTM E3173-18)

3.12 **배치(Deployment)**: 시스템이 운영되고 상태전환(Cutover)에 연관된 문제가 해결되는 프로젝트의 단계(ISO/IEC/IEEE 24765:2010)

3.13 **수명 종료 또는 단종 (EOL: End of Life)**: 제조업체가 제조업체에서 정한 사용 연수를 초과한 제품을 더 이상 판매하지 않고, 사용자에게 통지하는 절차를 포함한 공식적인 EOL 과정을 진행함으로써 시작되는 제품의 수명 주기 단계

참고: 수명 종료 시점이 되면 TPLC의 제한적 지원 단계가 시작된다.

3.14 **지원 종료(EOS: End of Support)**: 제조업체가 모든 서비스 지원 활동을 종료하고 서비스 지원이 해당 시점을 넘어 연장되지 않아 시작되는 제품의 수명 주기 단계

참고: 지원 종료 시점이 되면 TPLC의 지원 종료 단계가 시작된다.

3.15 **필수 성능(Essential Performance)**: 기본 안전과 관련된 것들 이외의 제조업체가 정한 제한치를 초과하는 손실 또는 저하로 인해 허용할 수 없는 위험을 발생하는 임상적 기능의 성능(IEC 60601-1:2005+AMD1:2012)

참고: 필수 성능을 유지하기 위해 유지보수, 수리 또는 업그레이드(예: 안전 또는 사이버보안 수정)가 필요할 수 있다.

3.16 **익스플로잇(Exploit)**: 취약점을 통해 정보 시스템의 보안을 침해하는 정의된 방법(ISO/IEC 27039:2015)

3.17 **펌웨어(Firmware)**: 주 저장장치와 기능적으로 독립적인 방식으로 저장되는 명령어 및 관련 데이터의 정렬된 집합으로, 일반적으로 읽기 전용 메모리(ROM)에 저장됨(ISO/IEC 2382:2015)

3.18 **무결성(Integrity)**: 데이터가 생성, 전송 또는 저장된 이후 무단으로 변경되지 않은 속성(ISO/IEC 29167- 19:2016)

3.19 **레거시 의료기기(동의어: 레거시 기기)(Legacy Medical Device, syn. Legacy Device)**: 현재의 사이버보안 위협으로부터 합리적으로 보호할 수 없는 의료기기

3.20 **수명 주기(Life cycle)**: 제품 또는 시스템의 초기 구상부터 최종 폐기 및 처분에 이르는 일련의 모든 수명 단계(ISO 81001-1:2021)

3.21 **환자 피해(Patient Harm)**: 환자의 신체 부상 또는 건강 손상(ISO/IEC 지침 51:2014에서 수정됨)

3.22 **환자 안전(Patient Safety)**: 환자의 건강에 대한 허용할 수 없는 위험으로부터의 자유(ISO/IEC 지침 51:2014에서 수정됨)

3.23 **개인정보 보호(Privacy)**: 해당 개인에 대한 부당하거나 불법적인 데이터 수집 및 사용으로 인한 개인의 사생활이나 일에 대한 침해를 받지 않는 상태(ISO/TS 27799:2009)

3.24 **제품(Product)**: 조직과 고객 간에 어떤 트랜잭션 없이도 생산될 수 있는 조직의 산출물(ISO 81001-1:2021)

3.25 **복원력(Resilience)**: 결함이나 오류가 발생했을 때 필요한 기능을 계속 수행할 수 있는 기능 단위의 능력(ISO/IEC 2382:2015)

3.26 **위험 관리(Risk Management)**: 위험을 분석, 평가, 통제 및 모니터링하는 업무에 관리 정책, 절차 및 실무를 체계적으로 적용하는 것(ISO/IEC 지침 63:2019)

3.27 **위험 이전(Risk Transfer)**: 위험 요소 관리에 대한 책임을 위험 요소를 더 잘 완화할 수 있는 다른 조직이나 기능적 주체에 이전(ISO/IEC/IEEE 24765:2017)

3.28 **보안 정책(Security Policy)**: 1. 각 프로젝트 조직 수준에서 알아야 할 필요성 및 정보 접근에 대한 규칙 2. 하나 이상의 개체 집합의 하나 이상의 활동을 제한하는 규칙 집합(ISO/IEC 10746-3:2009)

3.29 **보안 테스트(Security Testing)**: 권한이 없는 사람이나 시스템이 테스트 항목과 관련 데이터 및 정보를 사용, 읽기 또는 수 정할 수 없고 권한이 있는 사람이나 시스템이 이에 대한 접근을 거부당하지 않도록 보호되는 정도를 평가하기 위해 수행되는 테스트 유형(ISO/IEC/IEEE 29119-1:2013)

3.30 **소프트웨어 자재 명세서(SBOM: Software Bill of Materials)**: 하나 이상의 식별된 컴포넌트, 컴포넌트 간의 관계 및 기타 관련 정보의 목록

참고: 종속성이 없는 단일 컴포넌트에 대한 SBOM은 해당 컴포넌트의 목록일뿐이다. ‘소프트웨어’ 는 ‘소프트웨어 시스템’으로 해석될 수 있으므로 하드웨어(펌웨어가 아닌 실제 하드웨어)와 매우 낮은 수준의 소프트웨어(예: CPU 마이크로코드)도 포함될 수 있다.(미국 국가통신정보국(NTIA :National Telecommunications and Information

Administration), 소프트웨어 컴포넌트 투명성 프레임워크: 공통 소프트웨어 자재 명세서(SBOM) 수립 2021-10-21).

3.31 **소프트웨어 컴포넌트(Software Component)**: 소프트웨어 시스템 또는 모듈, 단위(Unit), 데이터 또는 문서와 같은 요소를 지칭하는데 사용되는 일반적인 용어(IEEE 1061)

참고: 소프트웨어 컴포넌트에는 여러 개의 단위가 있거나 하위 수준의 소프트웨어 컴포넌트가 여러 개 있을 수 있다.

3.32 **서드파티 소프트웨어(Third-party Software)**: 관련 당사자와 독립적인 것으로 인정되는 개인 또는 단체가 제공하는 소프트웨어 (ISO/IEC 25051:2014에서 수정)

참고: 관련 당사자는 일반적으로 공급자(‘제1 당사자’) 및 구매자(‘제2 당사자’)의 이해관계이다.

3.33 **위협(Threat)**: 보안을 위반하고 피해를 줄 수 있는 상황, 기능, 조치 또는 사건이 있을 때 존재하는 보안 위반 가능성이 있는 상태(ISO/IEC 지침 120)

3.34 **위협 모델링(Threat Modeling)**: 시스템에 피해를 입힐 수 있는 파괴, 공개, 데이터의 수정 또는 서비스 거부 형태의 모든 상황 또는 사건을 노출시키는 탐색적인 과정(ISO/IEC/IEEE

24765-2017에서 적용)

3.35 제품 수명 전주기(TPLC: Total Product Life Cycle): 의료기기 수명 주기에서 개발, 지원, 제한적 지원 및 지원 종료 단계

참고: 일부 관할권에서는 다른 용어로 단계를 지칭할 수 있다.

3.36 업데이트(Update): 의료기기 소프트웨어에 대한 수정형, 예방형, 적응형 또는 진보형 수정 사항

참고 1: ISO/IEC 14764:2006에 설명된 소프트웨어 유지 관리 활동에서 파생된 개념

참고 2: 업데이트에는 패치 및 구성 변경 사항이 포함될 수 있다.

참고 3: 적응형 과 진보형 수정 사항은 소프트웨어의 개선 사항이다. 이러한 수정사항은 의료기기의 설계 사양에 포함되지 않았던 수정사항이다.

3.37 업그레이드(Upgrade): 의료기기 또는 의료기기 컴포넌트를 최신 버전 또는 더 나은 버전으로 교체하거나 추가 기능으로 교체

3.38 취약점(Vulnerability): 하나 이상의 위협에 의해 악용될 수 있는 자산 또는 통제 약점(ISO/IEC 27000:2018)

3.39 취약점 관리(Vulnerability Management): 소프트웨어 취약점을 식별, 분류, 우선순위 지정, 수정 및 완화하는 주기적인 실무

4.0 일반원칙

본 장에서는 의료기기를 개발, 규제, 사용, 모니터링할 때 모든 이해관계자가 고려해야 할 레거시 의료기기에 대한 일반 원칙을 제공한다. 이 지침 문서 전체에서 확인할 수 있는 일반 원칙은 레거시 의료기기를 포함하는 전 세계 의료시스템의 사이버보안 자세를 개선하는데 기초가 된다.

4.1. TPLC 프레임워크

사이버보안 위협 및 취약성과 관련된 위험은 개발부터 EOS에 이르기까지 의료기기 수명의 모든 단계에 걸쳐 고려되어야 한다. 실제로 임상 수명은 EOS 이후에도 연장될 수 있으며, HCP가 EOS 이후에도 의료기기를 계속 사용하기로 할 경우 EOS 이후 어느 시점에 폐기가 이루어질 수 있다. 많은 경우의 의료기기 임상적 유용성이 지원 가능성보다 더 높다고 알려져 있다. 모든 이해관계자는 의료기기의 사이버보안을 위해 개발, 지원, 제한적 지원 및 EOS의 TPLC 단계를 포함하는 계획된 수명 주기를 가져야 함을 인식해야 한다.

제한적 지원은 MDM과 HCP가 최종적으로 지원 종료 또는 제품 업그레이드/교체로 전환할 수 있도록 조정하고 준비하기 위한 전환기이다. EOS는 주로 의료기기의 사이버보안에 대한 책임이 HCP로 이전되는 시점으로 간주한다. EOS 이후에도 MDM은

관할지역의 규정에 따라 특정 시판 후 활동에 대한 책임이 있을 수 있다(자세한 내용은 7.2.1.3.항 참조). MDM과 HCP가 각 수명 주기 단계에 적절히 대비할 수 있도록 의료기기 EOS에 이르기까지의 의사소통, 위험 관리 및 책임 이전과 관련된 다양한 활동이 시간이 지남에 따라 발생할 것이다.

4.2. 의사소통

위협으로부터 효과적으로 보호하기 위해서는 이해관계자 간의 개방적이고 투명한 의사소통이 필요하다. MDM은 EOL 및 EOS에 대한 계획을 세우고, 가능한 한 빨리 EOL 및 EOS 예상 시기를 알리기 위해 노력해야 하며, 의료기기 구매 및 설치의 일부로서 알리는 것도 좋다. 사용자는 조기 인지를 통해 MDM으로부터 의료기기 유지 관리와 관련된 다음 단계를 안내받음으로써 EOL 및 EOS 날짜를 적절하게 계획할 수 있게 된다. 이 정보를 통해 HCP는 의료기기를 폐기하거나 의료기기에 대한 보안 유지의 추가적인 책임을 갖게 된다.

이 문서 전반에 걸쳐 MDM 또는 HCP의 의사소통과 관련된 권장 사항은 해당 당사자 또는 다른 이해관계자 간의 적극적인 접촉 및 참여를 포함하는 것으로 이해해야 한다. 제공되거나 전달되는 정보는 상대방에게 적극적으로 보내거나, 상대방이 그러한 정보를 검색할 수 있다는 사실을 적극적으로 인지할 수 있도록 해야 한다. 적극적인 통지 없이 수동적으로 정보를 제공하는 의사소통 정책과 절차는

권장되지 않으며 가능하다면 기피해야 한다.

4.3. 공유 위험 관리

의료기기 사이버보안은 이해관계자, 특히 MDM과 HCP 간의 공동 책임이다. 이러한 공동 책임은 레거시 의료기기의 경우 특히 중요하다.

레거시 의료기기에 대한 위험을 적절히 관리하기 위해 MDM은 지원 단계에서 사이버보안을 최적화하고 향후 EOS 이후 보안 위험을 최소화하는 방식으로 의료기기를 설계해야 한다. MDM은 이 문서의 7, 8, 9장에 설명된 대로 의료기기를 지원해야 한다. HCP는 MDM과 적극적으로 협력하여 SBOM을 획득하고, MDM이 권장하는 적절한 사이버보안 보호 조치하에서 의료기기가 운용되도록 보장하고(관련 IT 인프라 포함) 해당 사이버보안 보호 조치가 유지 관리되는지 보장하며, 의료기기의 EOS 날짜를 계획해야 한다. MDM이 더 이상 지원하지 않는 의료기기는 현재 및 미래의 위협에 대해 취약해질 수 있으며, HCP는 해당 의료기기를 MDM이 지원하는 모델로 업그레이드하는 것을 고려해야 한다. SBOM에 대한 추가 정보는 IMDRF/CYBER WG/N73을 참조하면 된다.

5.0 의료기기 사이버보안을 위한 IMDRF TPLC 프레임워크 개요

사이버보안 위험의 동적 특성을 효과적으로 관리하기 위해서는 TPLC의 다양한 부분(설계, 제조, 테스트 및 시판 후 모니터링 활동을 포함하되 이에 국한되지 않음)에서 사이버보안 위험을 평가하고 완화하는 위험 관리가 TPLC 전반에 적용되어야 한다. 안전성과 보안 사이의 균형이 필요하다고 인식되고 있으며, MDM이 사이버보안 통제와 완화를 TPLC에 통합할 때에는 의료기기의 안전성과 기본 성능이 유지되도록 보장하는 것이 중요하다.

IMDRF N60 지침은 레거시 의료기기 사이버보안을 TPLC 4단계(개발, 지원, 제한적 지원, EOS(그림 1))의 맥락에서 설명하고 있다. 일부 관할지역에서는 각 단계를 다른 용어로 지칭할 수 있으나, 각 단계에 설명된 개념은 일반적으로 적용 가능해야 한다. 또한 TPLC 단계는 서로 다른 기간 동안 발생할 수 있음을 유의해야 한다(예: 지원 단계가 제한적 지원 단계보다 더 길 수 있음).

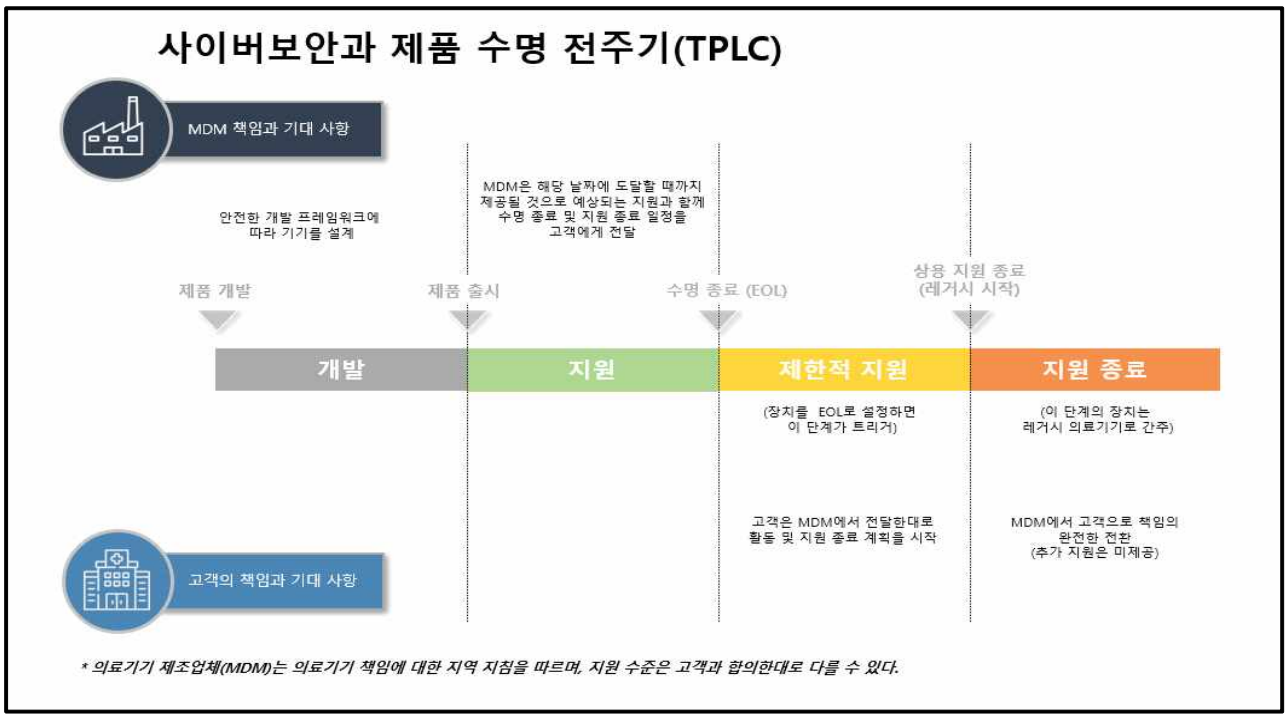

그림 1: 사이버보안을 위한 TPLC 기능으로서의 레거시 의료기기 개념 프레임워크

그림 1 참고: 또한 이 문서의 맥락에서 '고객' 이라는 용어는 'HCP'를 의미하는 것으로 이해해야 한다.

5.1. 개발(단계 1)

개발 단계(단계 1)는 MDM이 제품 설계부터 보안을 통합해야 하는 시장 출시 전 단계이다. MDM은 의료기기가 수명 주기 동안 안전하고 효과적으로 작동할 수 있도록, 위험 평가(Risk Assessment)를 수행하고, 위협을 식별하고, 보안 검증을 실행하고, 위험을 완화하여야 한다. 개발 단계의 또 다른 결과물은 사용자가 의료기기를 보안에 안전하게 운영할 수 있도록 지원하는 제품 관련 보안 문서 세트이다. 제품 개발 모범 실무(Best Practices)는 이 문서의 범위를 벗어난다. 확립된 표준에 대한 참조로서 다음이

포함되지만 이에 국한되지는 않는다:

- IEC 62443-4-1(TPLC)
- IEC 62443-3-2(보안 위험 평가)
- NIST 800-12
- NIST 시큐어 소프트웨어 개발 프레임워크
- IEC 81001-5-1: 2021
- IEC TR 60601-4-5: 2021
- IEC TR 80001-2-8:2016
- IEC 62443-4-2:2019

추가적인 표준들에 대해서는 IMDRF/CYBER WG/N60 지침을 참조하면 된다.

5.2. 지원(단계 2)

지원 단계(단계 2)에 있는 의료기기는 다음과 같은 의료기기로 정의된다:

1. 환자 치료에 사용되고 있는,
2. 시장에서 판매 중인,
3. 공급업체가 지원하는 주요 소프트웨어, 펌웨어 또는 프로그래머블 하드웨어 컴포넌트들(예: CPU) 을 포함.

단계 2의 의료기기는 전체적인 사이버보안 지원(즉, 소프트웨어

패치, 소프트웨어와 하드웨어 업데이트, 및 적절하다고 판단되는 지원)을 받아야 한다.

이 카테고리에 속하는 의료기기는 시장에서 '최신' 또는 '최첨단'으로 간주하며, 의료기기의 설계에 포함된 광범위한 보안 기능을 제공할 수 있다. 의료기기의 설계에 보안 모범 실무가 통합된 정도에 따라 MDM이 이 문서에 설명된 지원 실무를 얼마나 쉽게 준수할 수 있는지 결정된다.

이 단계에서 확립된 주요 실무는 조정된 취약점 공개 절차(이하 CVD: Coordinated Vulnerability Disclosure)를 통한 취약점 식별 및 알림이다. 지원 계약에 따라 MDM은 추가 서비스(예: 보안 모니터링, 백업/복구 등)의 제공을 통해 보안을 지원할 수도 있다. 모든 단계 2의 지원 실무가 레거시 진행의 다음 단계로 이어지지는 않는다.

5.3. 제한적 지원(단계 3)

제한적 지원 단계(단계 3)에 속하는 의료기기는 다음과 같은 의료기기로 정의된다:

1. 환자 치료에 사용되고 있는,
2. MDM에 의해 EOL로 선언되었고, 현재 해당 MDM에서 마케팅 또는 판매되지 않으며,
3. a) 개발자가 지원하지 않고 b) 의료기기 안전 및 효율성에 대한 위험이 완화되어 현재 사이버보안 위협으로부터 의료기기를

합리적으로 보호할 수 있는 소프트웨어, 펌웨어 또는 프로그래머블 하드웨어 컴포넌트들(예: CPU)을 포함.

단계 3에서 MDM은 가능한 경우 해당 의료기기에 대해 사이버보안 지원을 계속 제공해야 한다. 예를 들어, MDM이 소프트웨어에 대한 업데이트나 패치를 개발하는 것이 불가능할 수도 있지만, 가능한 경우 서드파티 컴포넌트 또는 소프트웨어 패치를 계속 적용해야 한다.

이 범주에 속하는 의료기기는 설계 내에 다양한 보안 기능이 포함될 수 있다. 제품 설계에 보안 모범 실무가 통합된 정도에 따라 MDM이 지원 단계에서 설명된 지원 실무를 얼마나 쉽게 준수할 수 있는지가 결정된다.

MDM은 사용자에게 제한 사항의 영향을 받는 의료기기 및 서비스, 완화되지 않은 것으로 보이는 보안 위협들, 그리고 HCP에 의해 구현되어야 하는 보안 보호 요소들을 알려야 한다.

단계 3의 의료기기는 단계 2의 의료기기에 비해 네트워크 통제와 같은 추가적인 보상 통제가 필요한 경우가 많이 있다. 단계 3에서 MDM 및 제공업체는 합리적으로 달성할 수 있는 모든 단계 2의 실무를 계속 따라야 한다.

5.4. EOS(단계 4)

EOS 단계(단계 4)에 속하는 의료기기는 다음과 같은 의료기기로 정의된다:

1. 환자 치료에 사용되고 있는,
2. MDM에 의해 EOS로 선언되었고, 현재 해당 MDM에서 마케팅 또는 판매되지 않으며,
3. a) 개발자가 지원하지 않고 b) 의료기기 안전 및 효율성에 대한 위험이 완화되지 않아 현재 사이버보안 위협에 대해 의료기기를 합리적으로 보호할 수 없는 소프트웨어, 펌웨어 또는 프로그래머블 하드웨어 컴포넌트들(예: CPU)을 포함.

MDM은 의료기기가 4단계에 진입하기 전에 더는 의료기기에 대한 지원을 보장할 수 없음을 사용자에게 알려야 한다. 이러한 의사소통은 사용자가 상속받을 수 있는 잠재적 위험과 완화 전략, 업그레이드 기회에 대한 식별을 포함해야 한다.

모든 의료기기는 결국 EOS에 도달하게 된다. 사이버보안 EOS를 넘어서는 의료기기의 보안에 안전한 사용은 배치 환경의 보안 기능에 크게 좌우되므로 이러한 상황에 대비하는 것은 MDM과 고객 간의 공동 책임이다.

5.5. 수명 주기 단계의 전환을 초래하는 위험 평가 프레임워크

의료기기와 해당 의료기기의 소프트웨어, 그리고 기타 디지털 컴포넌트들은 시간이 지남에 따라 EOL/EOS에 도달한다. 의료기기가 판매될 때 서드파티 소프트웨어 컴포넌트의 지원 수명은 의료기기의 EOS 수명보다 더 짧다고 알려졌을 수도 있고, MDM이 발표한 의료기기의 EOS보다 한참 전에 갑자기 지원 중단이라고 선언될 수도 있다. MDM은 서드파티 소프트웨어 컴포넌트의 지원에 대해 사전에 인지하고 있다면, 의료기기의 설계 때 해당 컴포넌트의 단계 전환으로부터의 위험을 해결하기 위한 적절한 계획을 마련해야 한다. 컴포넌트들의 갑작스럽고 동기화되지 않은 EOL/EOS 선언과 상태 변환 탓에 발생할 수 있는 위험을 관리하기 위해, MDM은 수명 주기 단계의 전환을 초래할 수도 있는 위험을 평가하는 다음의 프레임워크를 활용할 수 있다:

1. 의료기기 내의 단일 컴포넌트가 EOL/EOS가 되면, MDM은 의료기기에 대한 위험 평가를 수행하고, 환자 안전 위험이 발생하는지, 발생한다면 어떤 종류의 위험인지를 판단한다
    a. 환자 안전에 영향을 미치지 않는 경우, 의료기기는 현재 수명 주기 단계(즉, 지원 또는 제한적 지원)로 유지되며, 사용자에게 해당 컴포넌트가 EOL/EOS에 도달했음을 알린다.
2. 만약 환자의 안전에 영향이 있고, 의료기기가 지원 단계에 있는 경우, MDM은 지원이 되지 않는 컴포넌트의 위험을 완화하려는 시도(예:

업데이트 또는 기타 설계 변경)를 해야 한다. 지원 단계에 있는 경우, 업데이트 또는 설계 변경의 목표는 지원되지 않는 컴포넌트의 기능을 지원되는 대체 컴포넌트 또는 기타 설계 변경으로 대체하여, 의료기기가 계획된 EOS에 도달할 때까지 의도된 용도를 보안에 안전하게 유지할 수 있도록 하는 것이다. MDM의 위험 평가와 더불어 더 넓은 부문에서의 관련 위협 정보를 통해 이 시점에서의 단계 전환 적절성 여부를 결정하는데 도움을 주어야 한다

a. 만약 지원되지 않는 컴포넌트의 사용 없이 위험이 완화되어 의료기기를 합리적으로 보호할 수 있는 경우, 해당 의료기기는 지원 단계에 그대로 남아있을 수 있다.

b. 만약 의료기기가 합리적으로 보호될 수 있도록 위험이 완화되었지만, 완화 조치에 지원되지 않는 컴포넌트가 포함된 경우, MDM은 의료기기를 제한적 지원 단계로 전환해야 한다. 지원되지 않는 컴포넌트를 활용하는 완화 조치 사용은 모범 실무로 고려되지 않으며 최후의 수단으로 사용해야 한다. MDM은 이러한 단계 전환을 공개적으로 알리고 전환을 용이하게 하는 데 필요한 자세한 보안 문서를 제공해야 한다. (이 의사소통에 관한 자세한 내용은 8.1.1.5.항을 참조한다.)

3. 만약 환자의 안전에 영향을 미치고, 의료기기가 제한적 지원 단계에 있는 경우, MDM은 지원되지 않는 컴포넌트의 위험을 완화하려는 시도(예, 설계 변경 또는 보상 통제)를 해야 한다. MDM의 위험 평가와

더불어 더 넓은 의료 부문의 관련 위협 정보를 통해, 이 시점에서의 TPLC 단계 전환 적절성 여부를 결정하는데 도움을 을 주어야 한다.

a. 만약 의료기기를 합리적으로 보호할 수 있을 정도로 위험이 완화된다면, 해당 의료기기는 제한적 지원 단계에 남아있을 수 있으며, 사용자에게 해당 컴포넌트가 EOL/EOS에 도달했음을 알린다.
b. 만약 의료기기를 위험으로부터 합리적으로 보호할 수 없는 경우, 의료기기는 EOS 단계로 전환해야 하며, MDM은 이러한 전환을 공개적으로 알려야 한다. (이 의사소통에 대한 자세한 내용은 9.1.1.2항을 참조하면 된다.)

위의 프레임워크는 갑작스러운 서드파티 컴포넌트 EOL/EOS 선언을 위한 것이다. 일반적으로 의료기기 유지 보수를 위해 제공되는 소프트웨어 지원 수준은 의료기기 유지보수 계획에 명시되어 있다. 소프트웨어 컴포넌트의 EOS 날짜는 TPLC 전반에 걸쳐 의료기기 위험 관리에 도움이 되므로 SBOM에 포함될 수도 있다.

EOL/EOS 이후에도 의료기기를 계속 운영하기 위해 위험의 균형을 맞추는 방법에 대한 자세한 내용은 HSCC HIC-MaLTS의 책임 이전 프레임워크를 참조하면 된다.

6.0 개발 수명 주기 단계 : 책임/기대 사항

이 장에서는 의사소통, 위험 관리 및 책임 이전과 관련된 개발 수명 주기 단계의 이해관계자 책임에 대해 자세히 설명한다.

6.1. 의사소통

레거시 의료기기와 관련하여 가장 중요하고 잘 알려진 도전 중 하나는 정보 부족이다. 이러한 정보 부족은 의료기기의 보안 통제, 소프트웨어 공급망 또는 지원 상태와 같은 의료기기의 기술적 특징과 관련이 있을 수 있다. 또한, 정보 부족은 조직 내의 도전과도 연관 지어질 수 있는데, 즉, 조직 내에(MDM 및 HCP) 어느 당사자가 해당 의료기기의 지속적인 유지보수를 책임지는지, 보안 상태에 대한 정보를 언제, 어떻게, 누구에게 전달할 것인지 등의 문제이다. 결과적으로 레거시 의료기기와 관련하여 MDM, HCP 및 기타 관련 당사자 간의 의사소통이 필수적이다. 이러한 필요성을 해결하기 위해 조직은 의료기기 TPLC의 여러 단계에서 레거시 의사소통 전략을 수립하고 시행해야 한다.

6.1.1. MDM 권장 사항

다양한 수명 주기 단계에서 HCP의 피드백은 미래의 의료기기 및 의료기기 업그레이드에 대한 MDM의 설계에 영향을 미칠 수 있다. 후속 TPLC 단계와 관련된 추가적인 의사소통 절에서는 HCP가 의료기기를 구매하고 배치한 후의 고려 사항을 다루는 권장 사항들을

제공한다.

6.1.2. HCP 권장 사항

HCP는 이 TPLC 단계에서 임상과 사이버보안에 대한 필요 사항과 기대 사항에 대한 피드백을 제공하여 MDM 의료기기 개발에 정보를 제공할 수 있다.

6.2. 위험 관리

6.2.1. MDM 권장 사항

1. 기본 보안 통제 : MDM은 의료기기의 수명 주기 동안 보안을 통합하고 유지 관리할 수 있는 방식으로 제품을 설계해야 한다. 이는 시큐어 개발 프레임워크를 사용하여 달성할 수 있다. 적절한 통제 영역과 구체적인 권장 사항은 다음을 포함한다.
    a. 의료기기의 의도된 사용방법에 따른 보안 설계 및 통제
        i. 보안 위험 평가
        ii. 위협 모델링
        iii. 보안 테스팅
        iv. 고객 대면 제품 보안 문서 및 의사소통
    b. 사이버보안 취약성과 기능에 대한 시판 후 모니터링
        i. 취약점 식별
        ii. 의료기기 보안 설계, 통제 및 완화를 기반으로 한 취약성 위험 식별

c. 의료기기의 보안 위험도에 기반한 보안 패치와 위험 완화 조치의 가용성 보장

i. 취약점 및 해당 완화 조치와 관련하여 영향을 받는 모든 사용자에게 조율되고 명확한 의사소통을 제공

ii. 보안 패치가 가용하지 않을 시 다른 완화 옵션의 식별

2. 서드파티 컴포넌트 고려사항: MDM은 컴포넌트에 대한 서드파티 벤더의 지원이 HCP에서 사용 중인 해당 의료기기의 수명 내에 종료될 수 있으며, 이는 의료기기의 보안에 안전한 운영을 지원하는 MDM의 능력에 악영향을 미칠 수 있음을 고려해야 한다.

6.2.2. HCP 권장 사항

HCP는 아직 구매 절차를 시작하지 않았으므로 HCP에 대한 위험관리 권장 사항은 현 단계에서는 적용할 수 없다.

6.3. 책임 이전

MDM이 아직 HCP에 의료기기를 제공하지 않았으므로 현 단계에서는 책임 권고 사항 이전이 적용할 수 없다.

7.0 지원 수명 주기 단계: 책임/기대 사항

본 장에서는 지원 수명주기 단계에서 의사소통, 위험 관리 및 책임 이전과 관련된 이해관계자들의 책임 사항에 대해 자세히 설명한다.

7.1 의사소통

이 장에서는 의료기기의 지속적인 보안에 안전한 운영을 보장하기 위해 의료기기 수명 주기의 지원 단계에서 HCP와 MDM이 교환해야 하는 다양한 유형의 의사소통에 대한 권장 사항을 제공한다. 특히 지원 단계에서의 의사소통은 포괄적이어야 한다는 점은 매우 중요하다. 이 단계에 진입할 때, 조직들은 어떤 문서와 기타 정보가 필요한지 그리고 언제 필요한가를 식별해야 한다. 그다음 이러한 요구 사항들을 상대 당사자에게 전달하고 합의해야 한다. 구체적인 문서 요구 사항은 조직들마다 다를 수 있지만, 다음 절들에서는 일반적인 권장 사항을 제공한다. 의료기기의 현재 보안 기능이나 누락된 보안 기능에 대한 한 가지 가능한 의사소통 전략은 IEC TR 60601-4-5에 설명되어 있다.

7.1.1 MDM 권장 사항

1. 제품 보안 문서 제공: MDM은 의료기기가 구매되고 배치되는 동안 HCP의 위험 관리를 지원하기 위해, 제품 보안 문서를 지원 수명 주기 단계의 시작 뿐만 아니라 단계의 전반에 걸쳐 제공해야 한다. 적절한 문서에는 다음이 포함될 수 있다.
    a. 의료기기 보안을 위한 제조업체 공개 진술서(이하 MDS2: Manufacturer Disclosure Statement for Medical Device Security)
    b. 소프트웨어 자재 명세서(이하 SBOM: Software Bill of Materials)(SBOM 모범 실무에 대한 자세한 내용은 IMDRF N73을 참조하면 된다.)
    c. 보안 테스트 보고서 요약, 서드파티 보안 인증서 또는 이와 유사한 문서
    d. 고객 보안 문서(예: 안전한 배치, 운영 및 서비스를 보장하기 위한 기술 지침 - 시스템에 대한 인터페이스, 통신 프로토콜, 네트워킹, 클라우드 또는 통신 종속성에 대한 정보를 포함)
2. TPLC문서 제공: MDM은 의료기기 구매 및 설치 절차의 일부로서 주요 수명 주기 이정표(사이버보안 EOL 및 EOS 날짜(예측이 가능하다면)를 포함)에 대해 명확하게 전달해야 한다. MDM은 이 정보를 가능한 한 미리 제공해야 한다. 현재의 실무에 따르면 HCP를 가장 잘 지원하기 위해 적어도 2년 전에 정보를 제공하는 것이 좋다. MDM은 다음 정보를 명확하게 전달함으로써 HCP와 사용자를 지원

할 수 있다:

a. 영향을 받는 의료기기
b. 의료기기의 운영 체제
c. 배치된 의료기기의 버전
d. 소프트웨어 컴포넌트들 식별
e. 서비스 변경 예정일
f. 서비스 변경 후 이용 가능한 유지보수 범위
g. 추가적인 보상 통제

3. 관련된 업데이트된 제품 보안 및 수명 주기 문서의 제공: 의료기기가 수명 주기 동안 계속 사용됨에 따라 이를 지원하는 제품 보안 또는 수명 주기 문서가 변경될 수 있다(6.1.1.절 개발 수명 주기 단계의 의사소통에서 논의되었음) 이 경우, MDM은 HCP가 새로운 위험 또는 변경된 위험에 대응하기 위해, 필요에 따라 의료기기에 대한 위험 관리 전략을 조정할 수 있게 하려고 관련된 업데이트 문서(전자 형식도 가능)를 HCP에 제공해야 한다.
4. 취약점 및 패치 정보의 제공: 취약점이 발견되면 MDM은 적절한 완화 조치(예: 소프트웨어 패치)를 포함하여 관련 취약점 정보를 제공해야 한다. 이때, 환자 피해나 의료기기 파손을 방지하기 위하여, 시기적절한 의사소통이 필요한 고위험도 취약점에 높은 우선순위에 두어야 한다. 또한, 완화 방법(예: OTA 업데이트, 설치를 위한 서비스 인력의 배치) 및 구현 지침을 의료기기 운영자에게 제공해야 한다.
5. 서드파티 컴포넌트에 대한 적극적인 의사소통 제공: 의료기기 내의

소프트웨어와 기타 디지털 컴포넌트가 의료기기 자체보다 먼저 EOL/EOS에 도달할 수 있따. 이 경우 해당 컴포넌트에 대한 지원이 부족하면 의료기기에 위험이 발생할 수 있다. 이러한 위험을 보상하기 위해 MDM은 다음을 수행해야 한다:

a. 의료기기 내에서 사용되는 서드파티 컴포넌트의 지원 상태를 추적
b. 서드파티 컴포넌트가 지원이 끊길 시 발생할 수 있는 위험을 평가
c. 새로운 위험과 사용 가능한 모든 완화 조치를 HCP에게 전달

6. 환자 의사소통 제공: 이 문서의 범위를 벗어나지만, MDM과 HCP는 모두 관련이 있는 경우 EOL/EOS날짜와 정보를 환자에게 전달해야 한다.

7.1.2 HCP 권장 사항

1. 정보 요구 사항 식별: 모든 의료기기(레거시 의료기기 및 기타 의료기기 포함)에 대해 HCP는 의료기기를 적절하게 유지 관리하고 보호하는데 필요하다고 판단되는 정보의 유형(아래에서 자세히 설명), 해당 정보를 언제, 어떻게, 어디서 수신해야 하는지, 그리고 누구에게 해당 정보를 제공해야 하는지 파악해야 한다.

a. 예를 들어, HCP는 특정 레거시 의료기기에 대해 의료기기가 업데이트를 받을 것인지, 업데이트에 걸리는 시간 그리고 예상되는 업데이트 시기를 이해할 필요가 있다. 이에 따라 HCP는 HCP의 보안 및 임상 엔지니어링 팀에 이러한 정보를

제공하여, 해당 팀이 적절한 운영 및 유지 관리 결정을 내릴 수 있도록 결정할 수 있다.

b. HCP가 운영 전략을 수립할 때 고려해야 할 한 가지 특정 분야 중 하나는 책임 이전이다. 때에 따라 HCP는 MDM이 선언한 EOL 또는 EOS 날짜가 지난 후에도 의료기기를 계속 사용한다. 의료기기의 안전하고 효과적인 사용을 보장하기 위해 HCP는 지원되지 않는 의료기기를 사용하는 위험에 관한 책임이 언제 한 당사자에서 다른 당사자로 이전되는지 MDM에게 사전에 문의해야 한다.

2. 구매 전 의사소통: HCP가 시설에서 의료기기를 사용하는 동안 의료기기의 보안을 관리할 수 있도록 준비하기 위해, 의료기기의 구매와 설치 전에 적절한 온보딩 및 관리를 지원하기 위해 MDM과 HCP 간에 정보를 공유해야 한다. HCP는 다음의 정보를 요청할 수 있다.
    a. EOL 날짜(알고 있는 경우)
    b. EOS 날짜(알고 있는 경우)
    c. 의료기기의 소프트웨어 컴포넌트에 대한 업그레이드 전략 (예: 운영 체제, 서드파티 소프트웨어, 애플리케이션 소프트웨어)
    d. 의료기기가 적절하게 작동하는데 필요한 포트 및 서비스
    e. 의료기기를 격리하고 기능을 유지하기 위해 사용할 수 있는 방화벽 규칙
    f. 악성코드 탐지 기능 및 적절한 정의(무엇을 검사할 수 있는지)
    g. 보안 스캔 기능 및 적절한 스캐닝 정의(어떻게 스캐닝하는지)

h. 보안 로깅 기능

I. 의료기기 백업과 복원 절차

j. 취약점 통보를 받기 위한 통보 방법

k. 관리 계정 및 특권 접근 관리 툴을 통한 관리 기능

3. 지속적인 의사소통: 의료기기가 설치되어 사용 중인 경우, 의료기기의 수명 주기 동안 적절한 운영 및 위험 관리를 보장하기 위해 MDM과 HCP간의 통신이 필요하다. HCP는 의료기기 수명 주기 동안 다음과 같은 의사소통을 할 준비가 되어 있어야 한다:

    a. 평가된 위험을 설명하는 취약성 공개와 함께, 적절한 경우 푸쉬 메커니즘을 통한 업데이트 제공

    b. 알려진 취약점의 위험을 컨트롤하기 위한 완화 조치 권장 사항

    c. 의료기기에 나타날 수 있거나 네트워크 모니터링의 결과로 나타날 수 있는 침해 표시

    d. 의료기기의 수명 주기 동안 기계 판독이 가능한 형식으로 업데이트된 SBOM

    e. EOS에 도달하기 전 가능한 한 빨리 최신이 아닌 소프트웨어 컴포넌트(예: 운영 체제, 서드파티 소프트웨어)를 처리할 수 있는 옵션

7.2 위험 관리

7.2.1. MDM 권장 사항

1. 서드파티 위험 관리: 의료기기가 수명 주기 단계 중 어느 단계에 있더라도 EOL이나 EOS에 도달한 컴포넌트가 내장되어 있을 수 있다. 위험 평가는 안전, 필수 성능 그리고 사이버보안에 대한 전반적인 영향을 결정해야 한다.

   지원되지 않는 컴포넌트에 악용 가능한 취약점이 있더라도 의료기기 내부 또는 외부에 악용 가능성을 크게 줄일 수 있는 다른 보상 통제 장치가 있을 수 있다. 예를 들어 네트워크 방화벽은 네트워크 취약점을 노출하는 의료기기의 네트워크 포트에 대한 접근을 차단하거나 통제된 제한 접근을 제공할 수 있다. 방화벽도 한 가지 선택가능한 옵션이지만, MDM은 의료기기의 취약점을 해결하고 위험을 통제하기 위해 방화벽 또는 세그멘테이션에만 의존하는 방법은 피해야 한다. 환자 치료에 영향을 미칠 수 있기 때문이다.

2. 의사소통 기대 사항: 의료기기의 EOL 날짜가 다가오면 MDM은 HCP 및 규제 기관에 EOL 및 EOS 날짜에 대한 명확한 의사소통을 제공하고, HCP가 EOS 수명 주기 단계를 계획할 수 있도록 적절한 정보를 제공해야 한다. 이 수명 주기 정보는 7.1.1.절에 명시된 정보 외에 업그레이드 옵션을 포함할 수 있다. 이러한 추가 정보는 의료

기기의 지속적인 사용을 위해 HCP의 필수 위험 관리 활동을 지원하는데 사용될 수 있다.

3. 시판 후 기대 사항: 의료기기 시판 후 MDM이 완료해야 하는 특정 활동이 있으며, 이러한 기대 사항은 의료기기 사이버보안을 위한 TPLC에도 적용된다. 구체적으로 이러한 기대 사항은 다음과 같다.
    a. 고객 불만 사항의 수집, 문서화 및 대응(서비스 포함)
    b. 규제 기관에서 요구하는 부작용/사건 보고(예: 의료기기 문제로 인한 사망, 중상을 초래했거나 해당사건이 재발할 때 사망 또는 중상을 초래할 수 있는 사건)
    c. 필요한 경우 현장 안전 시정 조치(예: 리콜, 수정, IFU 변경 등)를 수행
        i. 일부 경우(예: 수명 주기 단계에 따라)에는 규제 요구 사항에 따라 MDM이 공식적인 조치를 취하지 않고 사이버보안 취약점의 존재와 알려진 완화조치를 전달할 수 있다.
        ii. 환자에게 직접 연결되는 의료기기(예: 연속 혈당 측정기)의 경우, MDM은 관할 요건에 따라 리콜 및 제거 정보를 전달해야 한다.
    d. 취약성 관리를 포함한 사전 예방적 위험 관리(예: 툴, 자원 및 인력을 사용하여 의료기기 보안 및 안전성 위험에 영향을 미치는 보안 문제를 지속적인 모니터링, 처리 및 전달)
    e. 취약성 관리를 포함한 사후 대응적 위험 관리(예: 필요에

따라 중요한 보안 및 안전성 위험을 처리하고 전달하기 위해 툴, 자원 및 인력을 통합 사용)에 참여

4. 지속적인 모니터링: EOS까지 MDM은 의료기기의 위험 프로필에 변화가 있는지 계속 모니터링하고, 이러한 변화가 안전, 일정, 예산, 활동 또는 의료기기의 지속적인 사용에 영향을 미칠 수 있으므로, 이를 HCP 및 규제 기관에 알려야 한다. 제한적 지원 단계 동안에도 HCP가 여전히 지원이 가능한 컴포넌트에 대해 소프트웨어 업데이트를 받을 수 있는지는 MDM과 HCP 간의 구체적 계약과 MDM의 EOL 날짜 연장 능력에 따라 달라질 수 있다.

7.2.2. HCP 권장 사항

의료기기가 TPLC를 통해 계속 진행됨에 따라 위험성 및 취약성 관리에 대한 변화하는 필요성과 이러한 위험을 완화하기 위한 HCP의 모범 실무를 구현할 수 있는 방법을 고려하는 것이 중요하다. 진화하는 위협 환경을 고려할 때 조치와 실무를 변경하고 발전시킬 필요가 있다. 신중한 계획이 없다면 레거시 의료기기가 초래하는 위험과 잠재적 결과는 시간이 지남에 따라 증가할 것이다. 의료기기의 사이버보안은 공동의 책임이지만, 의료기기의 수명주기가 당사자 간 의사소통을 통해 공유한 EOL 및 EOS 날짜를 지남에 따라, HCP는 의료기기에 대한 보안 조치를 구현하는 데 더 많은 책임을 져야 할 수 있다.

1. 기본 보안 고려 사항: 기본 보안 권장 사항은 지원 단계에서 매우 중요해진다. HCP를 위한 기본 보안 권장 사항에는 다음이 포함될

수 있다:

a. 위험 평가 절차를 통해 의료기기의 중요성과 심각성을 평가하여 의료기기에 네트워크 보안 통제를 적용
b. 추가적인 네트워크 및 물리적 통제와 정기적인 모니터링이 필요할 수 있는 심각성이 있는 의료기기를 식별하기 위해 위험 평가를 수행
c. 지원 및 패치 권장 사항을 위해 MDM과 활발한 의사소통 유지
d. 모든 현재 자산과 데이터 흐름을 파악하고 향후 구성 변경을 추적하기 위해 구성 관리를 사용
e. 사이버 위생 및 취약성의 개선을 지원하는 IT 보안 모니터링 및 패치 절차를 유지 관리
f. 논리적 및 물리적 보안 통제를 통한 비인가 접근으로부터 보호
g. 사이버보안 교육 및 인식 제고 프로그램
h. 취약점 관리

2. 운영 환경 고려 사항: 적절한 의료기기 위험 및 취약성 관리는 특정 의료기기 및 운영 환경에 따라 다를 수 있다. 접근 통제 및 모니터링에 대한 고려 사항은 아래 문단에 설명되어 있다.

3. 접근 통제: 의료기기는 기능을 수행하는데 필요한 HCP 네트워크의 일부에만 접근하고 연결할 수 있어야 한다. 의료기기에 대한 접근

통제를 구현하면 의료기기와 주고받는 정보 및 명령의 흐름을 필요 이상으로 제한할 수 있다. 이러한 통제는 의료기기 유형, 기타 네트워크 기능, 의료기기의 TPLC 내의 위치에 따라 달라질 수 있지만 차세대 방화벽과 같은 기존 도구를 사용하면 정의된 규칙 집합을 기반으로 동적 네트워크 세그멘테이션(또는 세분화) 및 시스템 정책 시행이 가능하다.

4. 네트워크 세그멘테이션(또는 세분화): 보안 요구 사항과 비즈니스 요구에 따라 네트워크를 세분화할 수도 있다. 그러나 네트워크를 세분화하면 네트워크의 일부가 손상될 경우 네트워크에서 측면 이동이 제한될 수 있다. 네트워크 세분화를 구현하는 경우, 세분화(방화벽 사용 포함)가 의료기기의 기능에 어떤 영향을 미치는지 고려해야 한다.

   참고: 많은 의료기기가 임상 애플리케이션 및 전자 의료 기록(EHR: Electronic Health Record)와 통합되도록 설계 및 제작되었다. 네트워크 세그멘테이션 또는 방화벽을 통해 레거시 의료기기의 취약성을 통제하면 관리 부담이 발생하고 환자 치료의 부정적인 영향을 미칠 가능성이 있으며 의도한 통합 이점이 감소한다. 따라서 MDM은 의료기기의 취약성을 해결하고 위험을 통제하기 위해 세그멘테이션 또는 방화벽 사용에 전적으로 의존하지 않아야 한다.

5. 다중 인증(MFA: Multi-Factor Authentication) : 다중 인증을 구현하면 네트워크 또는 의료기기 기능에 대한 역할 기반 접근을 시행할 수 있다. 그러나 의료 환경의 맥락에서 인증 모드와 속도를 고려해야 한다.

6. 모니터링: 네트워크에서 의료기기의 활동을 모니터링하는 것은 HCP가 보안 침해를 예방하고 보안 침해가 발생한 경우 대응하는데 도움이 될 수 있다. 의료기기의 수명 주기 동안 HCP는 네트워크에 연결된 의료기기의 활동을 추적하고, 경우에 따라 잠재적 의료기기 오작동에 대한 정보를 제공할 수 있는 일종의 활동 모니터링 시스템을 구현해야 한다.

   참고: 이는 침입 탐지 시스템, 침입 방지 시스템, 시스템 로깅 또는 방화벽 로깅 시스템의 형태를 취할 수 있다. 보다 성숙한 사이버보안 태세를 갖춘 HCP의 경우 이러한 시스템을 보안 정보 및 사건 관리 시스템에 통합할 수 있다. 이러한 시스템은 의료기기의 의도된 용도에 영향을 미칠 수 있으므로 HCP는 이러한 시스템 사용과 관련하여 MDM과 적절히 협력해야 한다. 레거시 의료기기의 특성을 고려할 때, 특히 실시간 운영 체제를 사용하는 의료기기의 경우 의료기기 자체에 모니터링 소프트웨어를 설치 및 추가하는 것이 불가능할 수 있다. 그러나 외부 의료기기와의 정보 흐름을 모니터링할 수 있는 도구를 사용하면 적절한 의료기기 동작 정보를 수집할 수 있다.

7. 인벤토리 고려 사항: EOS에 대한 사전 계획은 EOS 날짜를 알고 있는지에 관계없이 의료기기를 설치하기 전에 구매 논의 중에 시작된다. 강력한 인벤토리 관리 시스템을 사용하면 도움이 될 수 있다. 사용하기 쉽고 정확한 실시간 인벤토리를 통해, HCP는 다가오는 EOS 날짜를 사전에 계획할 수 있는 충분한 시간을 확보할 수 있다. 인벤토리에 있는 각 자산에 대해 다음과 같은 정보를 포함하면 도움이 될 것이다:
    a. 현재 수명 주기 단계
    b. 예상 EOS 날짜
    c. SBOM(SBOM 모범 실무에 대한 자세한 내용은 IMDRF N73 참조)
    d. 취약성 상태 및 소프트웨어 패치 상태
    e. 운영 환경(네트워크 다이어그램)
    f. 유지 관리 일정

가능한 경우 특정 작업을 자동화하면 의료진이 의료 서비스 제공에 집중할 수 있다. HCP가 EOS 날짜 이후에도 의료기기를 계속 임상적으로 사용하기로 결정한 경우에도 이러한 강력한 인벤토리 관리 시스템이 필수적이다. EOS를 계획하는 동안과 그 이후에도 의료기관은 의료기기를 계속 사용하는 데 따르는 위험을 이해하고 수용해야 한다. HCP는 위험에 대한 보상 통제 조치를 통해 EOS 날짜 이후에도 레거시 의료기기를 사용하는 것과 새로운 의료기기

또는 업그레이드된 의료기기를 구매하는 것을 비교하는 정기적인 임상적 혜택/위험 분석을 수행하는 것을 고려해야 한다.

8. 취약성 관리 고려 사항: IMDRF N60 지침에 명시된 바와 같이, HCP는 의료기기 사이버보안 관리에 위험 기반 접근 방식을 채택하는 것을 고려해야 한다. 이 절차는 다음에 적용되어야 한다:
    a. IT 인프라의 개발, 유지 및 업그레이드
        i. 의료기기가 연결되는 네트워크를 고려하는 것이 중요하며, 모든 네트워크 설계 및 아키텍처는 네트워크에 존재할 수 있는 다양한 잠재적 의료기기(레거시 의료기기 포함)를 고려해야 한다. 여기에는 의료진이 필요할 때 적시에 도움을 제공하는데 방해가 되지 않으면서 의료기기 보안을 강화하는 제로 트러스트 아키텍처 프로토콜을 구현하는 것이 포함될 수 있다.
    b. SBOM 수집 및 사용
        i. 의료기기는 그 아키텍처 및 설계의 특성상 다양한 출처 및 공급업체의 소프트웨어와 하드웨어(임베디드 시스템, 데이터 로깅, 하드웨어 컴포넌트 등을 포함하되 이에 국한되지 않음)이 모두 포함될 수 있다. HCP는 네트워크 인프라에 통합된 모든 의료기기에 대해 SBOM을 요청하는 것이 중요하다. 가능한 경우 SBOM을 통해 고객은 해당 의료기기가 TPLC를 통해 어떻게 진행될 수 있는지와 위험 통제 조치 및 완화 전략을 보다 효과적으로 적용하는 방법을 더 잘

이해할 수 있게 된다.

ii. 일부 유형의 소프트웨어 또는 하위 시스템에는 이를 컴포넌트로 포함하는 모든 시스템에 영향을 미치는 취약점이 있는 경우가 드물지 않다. SBOM을 통해 HCP는 의료기기 자체가 아닌 의료기기의 컴포넌트와 관련된 공개된 취약점의 영향을 받을 수 있는지 확인할 수 있다.

iii. 의료기기가 EOL 및 EOS 날짜에 가까워질수록 HCP는 공개된 취약점과 해당 취약점이 사용 중인 의료기기에 어떤 영향을 미칠 수 있는지 모니터링할 수 있는 시스템을 갖추는 것이 중요하다.

c. 네트워크에 새 의료기기 통합 및 설치

i. 새 의료기기는 기존 네트워크에 통합하기 전에 위험 평가를 받을 수 있다. 여기에는 네트워크 세그먼트에 의료기기를 위치시킬지 여부 결정, 접근 통제의 적용, 그리고 의료기기 활동에 대한 네트워크 모니터링의 통합 등이 포함될 수 있다.

d. 네트워크에 연결된 모든 장비(의료기기 및 노트북, 서버와 같은 연결된 장비를 포함하되 이에 국한되지 않음)에 대한 업데이트/변경.

IMDRF N60 지침에는 HCP가 위험 관리 절차를 적용할 때 참조할 수 있는 몇 가지 권장 표준이 제시되어 있다.

HSCC HIC-MaLTS ‘도전 과제 및 권장 사항’ 장에는 인벤토리 관리 및 SBOM을 포함하여 이러한 여러 과제를 해결하기 위한

구체적인 권장 사항이 포함되어 있다.

9. 폐기 고려 사항: IMDRF N60 지침의 6.6.2.절에는 의료기기의 TPLC에 대한 여러 가지 보안 권장 사항이 명시되어 있다. 의료기기가 EOS에 가까워지면 HCP는 의료기기 폐기를 검토하거나 지속적인 사용에 대한 사이버보안 위험을 가정하는 것이 중요하다.

7.3. 책임 이전

제품이 노후화되고 TPLC를 통과함에 따라 지원 및 제한적 지원 단계의 MDM/HCP 보안 책임 공유에서 EOS 단계의 사이버보안 지원 책임이 HCP 이전으로 전환되는 시점을 파악하는 것이 중요하다. 의료기기의 컴포넌트가 예기치 않게 지원이 끊어진다고 선언되는 경우를 제외하고, EOL 선언은 MDM/HCP 조정을 위한 과도기 역할을 하는 제한적 지원 단계로의 전환을 초래하게 된다. 다른 수명 주기 단계로의 전환에 대한 자세한 내용은 5.5.절을 참조한다. 7.3.절에서는 이러한 수명 주기 책임 이전을 구현하는 데 있어 MDM과 HCP 모두에게 권장 사항을 제공한다.

7.3.1. MDM 권장 사항

1. 타임라인 고려 사항: 모범 실무로서, 사이버보안 책임을 HCP로 이전하는 절차는 EOS가 시작되기 약 2~3년 전에 시작하는 것이 좋다. MDM이 HCP에게 2~3년 전에 통지를 제공하면 HCP가 의료기기 교체를 평가, 계획 및 예산을 수립하는데 도움이 된다.
2. 신규/업그레이드된 지원 의료기기로 전환하는 경로: 지원 단계가

종료되기 전에 MDM과 HCP는 최종적으로 EOS로의 전환 및/또는 제품 업그레이드/교체를 위해 조율하고 준비해야 한다. 지원되는 의료기기로 전환하게 되면 MDM과 HCP 간에 보안 책임을 공유하게 된다.

3. MDM에서 지원할 수 없고 HCP에서 교체하지 않은 의료기기의 경우 사이버보안 책임이 HCP로 이전된다. HCP가 사용할 수 있는 모든 옵션을 식별할 수 있도록 MDM은 다음 정보를 식별해야 한다:
    a. 제한적 지원 단계로의 전환 및 최종적으로는 EOS 단계로의 전환에 영향을 받는 의료기기에 대한 자세한 정보
    b. EOL/EOS에서 구현할 수 있는 구성 가능한 보안 옵션
    c. HCP에서 사용할 수 있는 업그레이드 옵션
        - 소프트웨어(S/W) 전용
        - 부분 - S/W 및 하드웨어(H/W)
        - 완전한 교체
            - o 교체 옵션 및 전략
            - o 사용 가능한 의료기기 모델 및 기능

7.3.2. HCP 권장 사항

지원 단계에서 HCP는 다음의 사항을 고려할 수 있다.

1. 사이버보안 및 임상 사용 관점에서 의료기기 관리 능력을 평가한다.
2. 기기 관리에 도움이 될 수 있는 서드파티의 지원 가능성을 파악한다.
3. 기기 교체 기회를 평가한다.
4. 기기를 지원하는 데 사용할 수 있는 추가적인 자원을 식별한다.

8.0 제한적 지원 수명 주기 단계: 책임/기대 사항

본 장에서는 의사소통, 위험 관리 및 책임 이전과 관련된 제한적 지원 수명 주기 단계의 이해관계자들 책임에 대해 자세히 설명한다.

8.1. 의사소통

제한적 지원 단계에서는 MDM과 HCP 간의 의사소통을 늘려야 한다. HCP에게 위험 정보를 제공하여 HCP가 이전받게 되는 위험에 대해 정보에 입각한 결정을 내릴 수 있도록 해야 한다. 완화 및 의료기기 교체 옵션에 대한 정보도 제공해야 한다.

8.1.1. MDM 권장 사항

1. 제한적 지원으로의 전환을 알리는 고객 통지 발표: MDM은 사이버보안 EOS 날짜까지 지원은 계속되지만 제한적 지원으로 전환되고, 사이버보안 EOS 날짜 이후에는 의료기기가 지원되지 않고 레거시 상태로 간주함을 알리는 고객 알림(예: 회사 웹사이트를 통한 공개 또는 HCP에 대한 직접 통지)을 발표해야 한다. 이러한 고객 의사소통 시기는 EOL 날짜가 다가올 때 이루어져야 하며, 이를 통해 의료기기 폐기 및 HCP의 비즈니스 연속성 계획에 대한 사전 통지가 가능하다.
2. 제한적 지원으로의 전환을 알리는 공개 정보 발표: MDM은 의료기기의 지원 상태를 설명하는 공개 알림(예: 회사 웹사이트 또는 기타 영구적으로 이용할 수 있는 자원을 통한 공개)을 발표해야 한다. 의료기기가

다른 단계로 이동하는 경우 이를 업데이트하여 관련 당사자(리셀러 및 잠재적으로 의료기기를 중고로 구매하려는 조직을 포함)이 해당 의료기기를 계속 사용할 경우 발생할 수 있는 잠재적 위험을 이해할 수 있도록 해야 한다.

3. 서비스와 문서의 지속적 제공: 실용적이고 적절한 한도 내에서 지원 단계(7.1.1.절)의 의사소통 서비스와 문서를 계속 제공한다. 여기에는 취약성 의사소통이 포함된다.
4. 수명 주기 계획 정보 제공: MDM은 고객이 EOS 및 관련된 고객 책임에 대비할 수 있는 충분한 시간을 가질 수 있도록 사이버보안 EOS 일정에 대한 타임라인을 지속해서 전달해야 한다. 가능한 의사소통에는 다음이 포함된다:
    a. 의료기기의 일부(예: 의료기기 소프트웨어)가 더 이상 지원되지 않을 때 일부 유지 관리가 중단되었음을 나타내는 주의 보안 통지 및 권고
    b. 보상 통제에 대한 의료기기별 정보 알림
    c. 수명 주기 단계의 변경으로 인한 의도된 사용 제한 사항
5. 제품 보안 문서의 제공: 지원 단계(7.1.1.1 및 7.1.1.3.항)에서 권장하는 보안 문서를 제공하는 것 외에도 MDM은 다음 문서를 제공해야 한다:
    a. 지원이 감소함에 따라 권장되는 보상 통제를 나타내는 업데이트된 보안 문서. 여기에는 다음이 포함될 수 있다:
        i. 방화벽
        ii. VPN

iii. 네트워크 격리

b. 기기 배치 환경에 대한 기대 사항

8.1.2. HCP 권장 사항

7.1.2.3의 의사소통은 계속되어야 하며, HCP는 수신되는 추가적이고 보다 세분화된 정보(예: 8.1.1)에 대해 궁금한 점이 있으면 MDM에게 문의해야 한다. HCP는 재판매 또는 중고 의료기기를 구매할지 여부를 평가할 수 있으므로 연장 계약 또는 서드파티 지원과 같은 추가 지원을 받을 수 있는지도 문의할 수 있다.

8.2. 위험 관리

8.2.1. MDM 권장 사항

MDM은 7.2.1.절의 지원 단계에서 시판 후 기대 사항 및 모니터링과 관련된 조치를 계속해야 한다. 그러나 위험 관리 활동의 일부로서 사전 취약성 관리와 관련된 노력의 빈도와 수준은 감소할 수 있다.

8.2.2. HCP 권장 사항

1. 재판매 또는 중고 의료기기 구매 여부를 평가할 때 EOL/EOS 위험을 고려: HCP는 재판매 또는 중고 의료기기를 구매할 수 있다. 이 경우 잠재적인 사이버보안 위험을 관리하기 위해 다음과 같은 조치를 취해야한다:

    a. 원하는 의료기기가 제한적 지원 중인지(즉, EOL 날짜가 도래한

상태인지) 아니면 EOS 상태인지 조사한다.

b. 그렇다면 HCP는 EOL/EOS 날짜가 도래한 의료기기 사용의 위험을 신중하게 고려해야 한다.

c. HCP가 의료기기를 구매하기로 결정한 경우에는 다음을 수행해야 한다.

i. 연장 계약 또는 서드파티 서비스 등을 통해 지원받을 수 있는지를 결정한다.

ii. 지원이 가능한 경우 HCP는 벤더 조직과의 계약에 지원을 요구하거나 포함하는 문구를 포함해야 한다. 벤더로부터 지원을 받을 수 없는 경우, HCP는 HCP가 의료기기를 지원하는 방법을 고려해야 한다.

2. EOS에 접근할 때 HCP를 위한 고려 사항

EOL 이후, HCP는 MDM의 적극적인 의사소통과 인벤토리 관리 시스템의 알림을 통해 의료기기의 EOS 날짜가 다가오고 있음을 통보받는다. HCP는 EOS에 대한 추가 준비를 해야 하며, 지원 없이 의료기기를 운용할 때의 위험이 적절히 통제되고 있는지 파악하는 데 도움이 되는 다음 질문들을 고려해야 한다. 아래 질문 목록은 완전한 목록은 아니다.

a. 예상 서비스 수명 이후 어느 기간 동안 의료기기를 임상 치료에 사용할 수 있을 것으로 예상되는가?

b. 기기를 임상 치료에 사용할 것으로 예상되는 동안 유지 관리 비용이 발생하는가?

c. 유지 관리 비용은 의료기 업그레이드와 어떻게 비교되는가?

d. 새롭거나 업그레이드된 의료기기가 어떻게 임상 치료를 개선하는 동시에 사이버 복원력을 향상할 수 있는가?

e. HCP는 이 의료기기의 보안을 유지할 수 있는 툴을 가지고 있는가?

f. HCP는 이 의료기기의 보안을 유지할 수 있는 재정적 자원을 보유하고 있는가?

g. HCP는 이 의료기기의 보안을 유지할 수 있는 전문 지식을 보유하고 있는가?

h. 이 의료기기가 손상될 경우 환자에게 어떤 위험이 발생하는가?

I. 이 의료기기로 인해 조직이 손상될 경우 환자에게 어떤 위험이 발생하는가?

j. 이 의료기기를 사용하지 않고 대체품으로 교체할 경우 환자에게 어떤 위험이 발생하는가?

k. 이 의료기기는 네트워크에 연결하지 않고도 유용하게 작동할 수 있는가?

l. 다른 어떤 통제 기능을 사용할 수 있는가?

추가 권장 사항 및 고려 사항에 대해서는 HCP가 HSCC HIC-MaLTS 내의 책임 이전 프레임워크를 참조할 수 있다.

8.3. 책임 이전

이 제한적 지원 단계는 MDM과 HCP가 최종적으로 지원 종료 또는 제품 업그레이드/교체로의 전환을 조정하고 준비하기 위한 과도기적 기간이다. 이 기간에 양 당사자는 의료기기 및 지원 옵션을 평가하고

미래 상태에 도달하기 위한 권장 사항을 제시한다. 이러한 전환 기간 공동의 보안 책임을 유지하기 위해 제한적 지원 계약을 이용할 수 있다. 제한적 지원의 이용 가능 여부와 범위는 다를 수 있으며 각 당사자가 이를 충분히 이해하고 인정해야 한다. 미래 상태가 변화되지 않고 지원이 끊긴 의료기기가 계속 서비스되고 MDM에서 지원할 수 없는 경우, 해당 의료기기의 지속적인 사용 및 관리를 지원하기 위한 보안 책임은 HCP에 있다.

사이버보안 지원 책임은 HCP로 이전된다. HCP가 특정 책임을 맡을 수 없는 경우, MDM은 가능한 경우 점진적인 책임 이전을 고려할 수 있다.

8.3.1. MDM 권장 사항

보안 책임을 HCP로 원활하게 이관하려면 다음 고려 사항 목록을 검토하고 평가해야 한다.

1. 고객이 사용할 수 있는 소프트웨어 업데이트를 모두 적용할 수 있도록, 사용할 수 있는 소프트웨어 업데이트를 식별한다(또는 EOL/EOS 마일스톤에서 고객에게 제공할 수 있음).
2. MDM이 제공하는 보안 문서는 HCP가 네트워크 보안 통제를 활성화하는 데 도움이 되는 정보를 제공해야 한다.
3. 의료기기 작동에 필요한 포트 및 IP 주소에 대한 HCP 정보를 제공하는 네트워크 요구 사항이 확인되어야 한다.
4. 네트워크 요구 사항을 통해 HCP는(네트워크에서) 의료기기에 접근

하는 불필요한 포트와 IP 주소를 모두 ‘강화’ 하고 차단할 수 있다.

5. 사용할 수 있는 제품 보안 문서(SBOM 포함).
6. 의료기기에 대한 사이버보안 모범 실무와 관련하여 이용할 수 있는 기타 정보를 통해 고객의 사이버보안 태세에 도움이 될 수 있다.
7. 다음을 포함하거나 포함하지 않을 수 있는 제한된 지원 옵션을 전달한다.
    a. 가능한 경우 하드웨어 컴포넌트 교체(예: 디스플레이 모니터, 캐비닛, 하드 디스크 드라이브 등)
    b. 소프트웨어 재 로딩, 의료기기 시스템 상태 복원
    c. 가능한 경우 네트워크 하드웨어 보안 장치의 추가(의료기기와 별도로)

8.3.2. HCP 권장 사항

보안 책임을 HCP로 원활하게 이관하려면 다음 고려 사항 목록을 검토하고 평가해야 한다.

1. 기기에 대한 사이버보안 모니터링
2. 취약점 관리
3. 물리적 및 논리적 접근 통제를 포함한 보상 통제 구현
4. 배치 환경이 EOS 의료기기를 적절히 보호하기에 적합한지 확인
5. 사고 대응 계획 실행
6. 비즈니스 연속성 계획 수립
7. HCP의 위험 관리 절차에 명시된 대로 정기적인 위험 평가 수행

9.0 EOS 수명 주기 단계: 책임/ 기대 사항

본 장에서는 의사소통, 위험 관리 및 책임 이전과 관련된 EOS 수명 주기 단계의 이해관계자 책임을 자세히 설명한다. EOS는 의료기기 수명 주기에서 중요한 이정표이며, HCP는 추가적인 사이버보안 책임이 이전되는 시점을 인지하고 그에 따라 준비해야 한다.

9.1. 의사소통

9.1.1. MDM 권장 사항

기기가 EOS 단계에 진입할 때, MDM은 HCP에 EOS 날짜와 의료기기가 EOS 단계에 도달할 시점을 알려야 한다. 이 단계에서는 추가적인 사이버보안 지원 책임이 HCP로 이전될 수 있다. HCP가 특정 책임을 맡을 수 없는 경우, MDM은 가능한 경우 점진적인 책임 이전을 고려할 수 있다.

1. 보안 유지 관리를 위한 제품 보안 정보 제공: MDM은 HCP가 MDM의 도움 없이 의료기기 사이버보안 위험을 가장 잘 관리할 수 있도록 관련 제품 보안 정보를 제공해야 한다. 이러한 정보에는 다음이 포함될 수 있다.
    a. 기기의 보안을 유지하기 위한 HCP의 추가적인 책임 사항 (사이트별 통제(예: 방화벽, 네트워크 격리, VPN)를 포함할 수 있다.)

b. 사이버보안 EOS 날짜 이후에 받을 수 있는 지원

c. 기기를 위한 사용 가능한 업그레이드 경로

d. 폐기 정보: MDM은 HCP가 향후에 의료기기를 폐기할 수 있도록 정보를 제공해야 한다.

2. EOS 단계로의 이전을 알리는 공개 정보 발표: MDM은 해당 의료기기의 지원 상태를 설명하는 공개 정보(예: 회사 웹사이트 또는 기타 영구적으로 이용할 수 있는 자원을 통한 공개)를 공개해야 한다. 리셀러 및 잠재적으로 중고 의료기기를 구매하려는 조직을 포함한 관련 당사자가 해당 의료기기를 계속 사용할 경우 발생할 수 있는 잠재적 위험을 이해할 수 있도록 업데이트해야 한다.
3. 시판 후 기대 사항의 일부로 접수된 환자 위험은 사후 취약성 관리를 통해 적절히 전달한다.

9.1.2. HCP 권장 사항

HCP는 EOS 초기(즉, 9.1.1.절)에 받은 정보에 대해 궁금한 점이 있으면 MDM에 문의해야 한다. HCP는 재판매 또는 중고 의료기기를 구매할지 여부를 평가할 수 있으므로 연장 계약 또는 서드파티 지원과 같은 추가 지원을 받을 수 있는지도 문의할 수 있다.

9.2. 위험 관리

9.2.1. MDM 권장 사항

EOS 이후에도 MDM은 관할 규정에 따라 특정 시판 후 활동에 대한 책임을 진다(7.2.1.3항 참조). 랜섬웨어 시나리오(예: 워너크라이 해킹)와

같이 환자 안전에 중대한 위험이 있는 경우 추가적인 대응 위험 관리 조치(7.2.1.3.항에 강조 표시된 것과 같은)가 필요할 수 있다.

9.2.2. HCP 권장 사항

1. 8.2.2.1.항에 설명된 대로 재판매 또는 중고 의료기기 구매 여부를 평가할 때 EOL/EOS 위험을 고려한다.
2. EOS가 지난 의료기기를 사용할 때 HCP를 위한 고려 사항: HCP가 EOS 날짜가 지난 의료기기를 사용하여 보안 위험을 감수한다면, 다음 사항들을 권장한다.
    a. 고위 경영진의 승인을 받은 강력하고, 자격을 갖추고, 적절한 자원(즉, 증가하는 위험을 관리 할 수 있는 자원)을 갖춘 사이버보안 프로그램을 구현해야 한다.
    b. 가능하면 자동화된 강건한 인벤토리 관리 시스템을 구현해야 한다.
    c. 진행 중인 조직 위험 관리 활동에 레거시 의료기기를 포함한다.
    d. 신뢰할 수 있는 정보 출처(정보 공유 분석 기관, 정보 공유 및 분석 센터, 컴퓨터 비상 대응팀(CERT: Computer Emergency Response Teams)와 같은 전파 기관, 규제 기관, 취약성 데이터베이스(예: 서드파티 컴포넌트에 대한 데이터베이스 등)를 사전에 모니터링한다.
    e. 네트워크 세그멘테이션, 사용자 접근 역할, 보안 테스트, 네트워크 모니터링, 네트워크 연결 해제 등의 대응책을 강화

한다.

f. 사용 가능한 대체 제품을 주기적으로 평가하고 EOS가 지난 의료기기를 운영하기로 한 결정을 재검토한다.

HCP는 추가 권장 사항 및 고려 사항에 대해서 HSCC HIC-MaLTS 내의 책임 이전 프레임워크를 참조할 수 있다.

9.3. 책임 이전

9.3.1. MDM 권장 사항

이 단계에서는 사용자에게 책임 이전이 완료된다. MDM은 해당 의료기기가 EOS이며 책임 이전이 완료되었음을 알린다.

9.3.2. HCP 권장 사항

책임/위험 수용 또는 새로운/업그레이드된 의료기기로 전환: 다양한 압력이 존재하는 상황에서, HCP가 의료기기의 기대수명을 초과하여 계속 사용하는 것은 드문 일이 아니다. 많은 경우 사용자는 의료기기가 고장 나거나 의도한 대로 작동하지 않아 내부 서비스 또는 폐기를 초래하게 된다. 다른 경우로서 위협으로부터의 방어 지원이 존재하지 않을 수도 있다. 두 경우 모두 환자에게 해를 끼칠 가능성이 존재한다. HCP는 반드시 강력한 인벤토리 관리 시스템을 갖추고 있어야 하며, 각 의료기기의 EOS 날짜가 다가오면 레거시 의료기기가 초래하는 위험과 조직 내 사이버보안 프로그램의 성숙도를 신중하게 고려해야 한다.

10.0 사이버보안 TPLC 요약: 책임/기대 사항

위의 6~9장에서는 사이버보안을 위한 4가지 TPLC 단계(개발, 지원, 제한적 지원 그리고 EOS)의 맥락에서 MDM과 HCP의 책임과 기대 사항에 대한 추가 세부 사항(의사소통, 위험 관리, 책임 이전 등)을 제공한다. 또한 위의 6~9장에는 의료기기 사이버보안을 위한 TPLC 전반에 걸쳐 의료기기 시판 후 MDM이 완료해야 하는 특정 활동에 관해 설명되어 있다. 그림 2에 표시된 요약 사이버보안 TPLC는 TPLC 전반에 걸쳐 책임 이전에 따라 주어진 책임과 기대 사항에 대한 노력의 수준을 표시한다.

사이버보안과 제품 수명 전주기(TPLC)

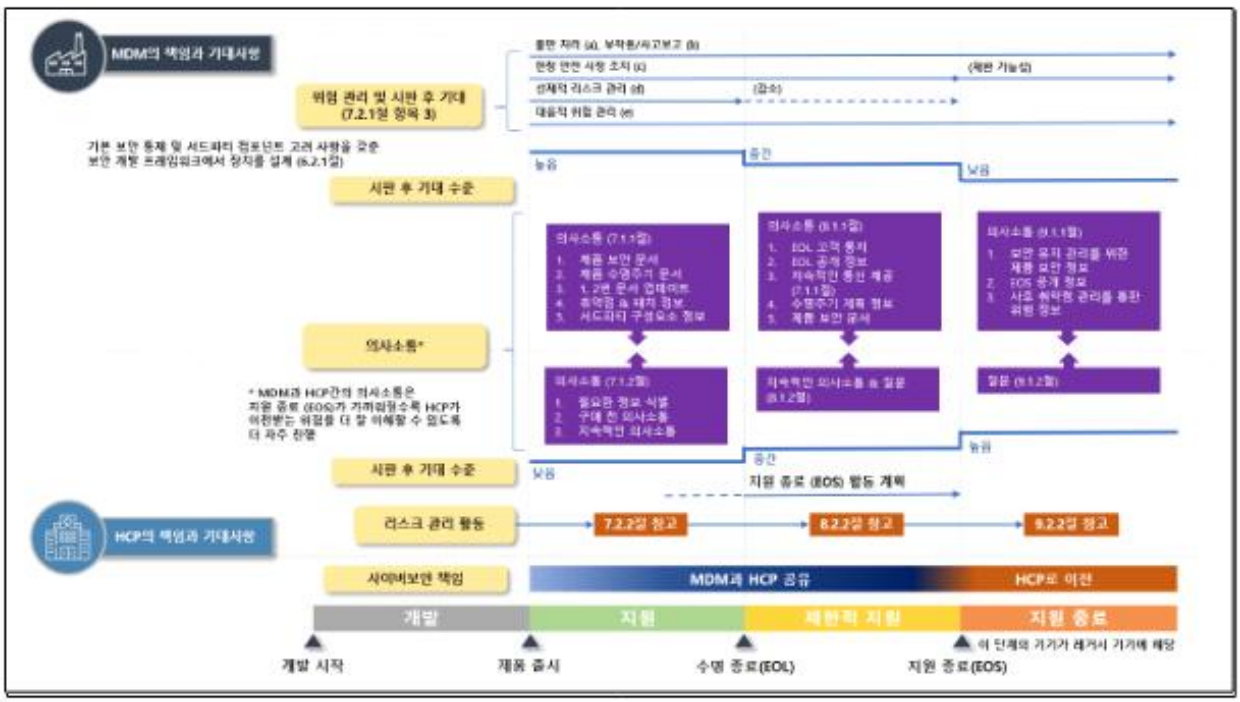

그림 2: 사이버보안을 위한 TPLC 기능으로서의 자세한 레거시 의료기기 프레임워크

11.0 의료기기 EOS 이후 보상 통제 관련 고려사항

보상적 위험 통제 조치(‘보상 통제’ 라고도 함)은 의료기기 설계의 일부로 구현된 위험 관리 조치 대신(또는 부재 시) 배치되는 특정 유형의 위험 통제 조치다(AAMI TIR97:2019). 건강 및 안전 위험 또는 기타 규정 미준수가 확인된 경우, MDM은 추가 수정, 시정 조치 및 해당하는 경우 예방 조치를 시행하여 의료기기를 규정 준수 상태로 만들어야 한다.

MDM이 의사소통을 통해 전달한 대로 의료기기가 EOS에 도달하면 HCP는 레거시 기술 사용에 따른 위험과 MDM의 보안 지원 부족에도 불구하고 의료기기를 계속 작동시키기로 결정할 수 있다. 계속 사용해야 하는 이유는 임상 치료의 의료기기를 사용할 기간이 지원되는 시간을 초과하는 경우, 시장에 사용할 수 있는 대안이 없는 경우, 또는 예산 제한이 있는 경우 등과 같지만 이에 국한되지 않는다.

HCP가 EOS 이후에도 의료기기를 계속 사용하기로 결정한 경우, 본 지침의 8장과 9장에 설명된 대로 제한적 지원 및 EOS 단계 동안 MDM에서 제공하는 제품 보안 문서를 참조해야 한다. 이 문서에는 의료기기 자체와 운영 중인 IT 환경에 적용할 수 있는 최소한의 보상 통제 조치가 포함되어 있다.

11.1. 보상 위험 통제 조치

보상 통제 조치를 구현하는 것은 기술 제공 및 자원 측면에서 HCP에 상당한 비용이 발생할 수 있다. 따라서 HCP는 위험 통제 조치를 보완하는 데 드는 비용과 새로운 의료기기를 구입하는 데 드는 비용 및 이점을 비교 및 고려해야 한다.

표 1에는 보상 통제에 대한 일반적인 권장 사항이 포함되어 있다. 이러한 권장 사항은 EOS의 맥락에서 제공되었지만 구현 가능성은 특정 의료기기와 운영 환경에 따라 달라지며 의료기기의 임상 및 의도된 용도를 손상하지 않아야 한다. 나열된 통제 조치는 완전한 것이 아니며 하나 이상의 통제 조치를 활용하거나 여러 가지 통제 조치를 조합하여 사용하는 것이 적절할 수 있다. 보상 위험 통제 조치를 구현할 때는 기술 혁신도 고려해야 한다.

통제 유형	위험 통제 조치 보상
물리적 접근	적절한 물리적 출입 통제 장치를 갖춘 제한 구역의 의료기기를 배치하여 권한이 있는 직원만 의료기기에 물리적으로 접근하도록 제한한다. 변조 방지 씰을 적절히 사용한다.
이동식 미디어	운영 체제 정책 또는 물리적 수단을 통해 시스템 기본 입력 출력 시스템/통합 확장 펌웨어 인터페이스 포럼(BIOS/UEFI)의 정책에 따라 USB 드라이브와 같은 이동식 미디어의 사용을 제한한다.
네트워크 격리	병원 네트워크에서 의료기기를 격리한다.
네트워크 분리	의료기기 및 의료기기가 통신하는 기타 인프라/서비스에 대한 가상 로컬 영역 네트워크(VLAN)를 설정한다.
모니터링	침입 탐지 시스템, 침입 방지 시스템 또는 보안 정보 및 사건 관리를 사용하여 의심스러운 활동이 있는지 의료기기와 네트워크를 모니터링한다.

원격 접근	의료기기에서 원격 접근 기능을 제거한다.
방화벽	기기를 물리적 또는 가상 방화벽 뒤에 배치하고 꼭 필요한 네트워크 통신에 대해서만 방화벽의 포트를 열어야 한다.
멀웨어 방지	MDM과 협의하여 의료기기에 안티멀웨어 솔루션을 설치한다. 네트워크에서 격리된 의료기기(독립형)의 경우, 인공지능(AI) 기반 멀웨어 방지 솔루션과 같이 정의 업데이트가 필요 없는 솔루션을 사용한다.
백업 및 복원	재해 발생 시 데이터 손실을 방지하기 위해 백업 및 복원 절차를 구현한다.

표 1: 위험 관리 조치를 보완하는 예시

11.2. 교육

기술적, 물리적 보상 통제 조치를 구현하는 것은 EOS 이후에도 의료기기의 보안을 유지하는데 도움이 될 수 있지만, 사이버보안 위협으로부터 HCP를 보호하려면 잘 훈련된 직원도 그에 못지않게 중요하다. 따라서 HCP는 사이버보안 교육을 제공하여 보안 의식을 고취하고 모든 사용자에게 사이버 위생 실무를 도입하는 것이 좋다. 여기에는 보안에 안전한 방식으로 의료기기를 작동하는 방법(예: 보안 네트워크에만 의료기기 연결)과 비정상적인 의료기기 동작(예: 무작위 종료/재시작, 보안 소프트웨어 비활성화)을 발견하고 보고하는 방법에 대한 교육이 포함되어야 한다. 또한 의료진에게 EOS 선언 후 의료기기의 보안 제한 사항과 의료기기 작동 시 위험을 완화하기 위해 준수해야 하는 보안 모범 실무에 대해 알려야 한다.

12.0 참고문헌

12.1. IMDRF 문서

1. 의료기기 사이버보안을 위한 소프트웨어 자재 명세서 원칙 및 실무 IMDRF/CYBER WG/N73FINAL:2020(2022년 4월)

2. 의료기기 사이버보안을 위한 원칙과 실무(IMDRF/CYBER WG/N60FINAL:2020(2020년 4월)

3. 소프트웨어 의료기기: 위험 분류 및 해당 고려 사항에 대한 가능한 프레임워크 IMDRF/SaMD WG/N12:2014(2014년 9월)

4. 의료기기 및 IVD 의료기기의 안전 및 성능에 대한 필수 원칙 IMDRF/GRRP WG/N47 FINAL:2018(2018년 11월)

12.2. 표준

5. AAMI TIR57:2016 의료기기 보안 원칙 - 위험 관리

6. AAMI TIR 97:2019, 의료기기 보안 원칙-기기 MDM을 위한 시장 출시 후 위험 관리

7. IEC 60601-1:2005+AMD1:2012, 의료용 전기 장비 - 파트 1: 기본 안전 및 필수 성능에 대한 일반 요구 사항

8. IEC 62304:2006/AMD 1:2015, 의료기기 소프트웨어 - 소프트웨어 수명 주기 절차

9. IEC 62366-1:2015, 의료기기 - 파트 1: 의료기기에 대한 사용성 엔지니어링의 적용

10. IEC 62443-3-2:2020, 산업 자동화 및 제어 시스템 보안 - 파트 3-2: 시스템 설계를 위한 보안 위험 평가

11. IEC 62443-4-1:2018, 산업 자동화 및 제어 시스템 보안 - 파트 4-1: 시큐어 제품 개발 수명 주기 요구 사항

12. IEC 81001-5-1:2021, 의료 소프트웨어 및 의료 IT 시스템 안전, 효과 및 보안 - 파트 5-1: 보안 - TPLC 내 활동

13. IEC 80001-1:2021, 의료기기를 통합하는 IT 네트워크에 대한 위험 관리 적용 - 파트 1: 연결된 의료기기 또는 연결된 건강 소프트웨어의 구현 및 사용 시 안전, 효과 및 보안

14. IEC TR 80001-2-2:2012, 의료기기를 통합하는 IT 네트워크에 대한 위험 관리 적용 - 파트 2-2: 의료 기 기 보안 요구 사항, 위험 및 통제의 공개 및 통신에 대한 안내서

15. IEC TR 80001-2-8:2016, 의료기기를 통합하는 IT 네트워크에 대한 위험 관리 적용 - 파트 2-8: 적용 지침 - IEC 80001-2-2에서 식별된 보안 기능을 설정하기 위한 표준에 대한 지침

16. ISO 13485:2016, 의료기기 - 품질 관리 시스템 - 규제 목적에 대한 요구 사항

17. ISO 14971:2019, 의료기기 - 의료기기에 대한 위험 관리 적용

18. ISO/TR 80001-2-7:2015, 의료기기를 통합하는 IT 네트워크에 대한 위험 관리 적용 - 적용 지침 - 파트 2-7: 의료 서비스 제공 기관(HCP)을 위한 IEC 80001-1 적합성 자체 평가 방법에 대한 지침

19. ISO/IEC 27000 제품군 - 정보 보안 관리 시스템

20. ISO/IEC 27035-1:2016, 정보 기술 - 보안 기술 - 정보 보안 사고 관리 - 파트 1: 사고 관리의 원칙

21. ISO/IEC 27035-2:2016, 정보 기술 - 보안 기술 - 정보 보안 사고 관리 - 파트 2: 사고 대응 계획 및 준비를 위한 지침

22. ISO/IEC 29147:2018, 정보 기술 - 보안 기술 - 취약점 공개

23. ISO/IEC 30111:2013, 정보 기술 - 보안 기법 - 취약점 처리 절차

24. ISO/TR 24971:2020, 의료기기 - ISO 14971 적용에 대한 지침

25. UL 2900-1:2017, 네트워크 연결 가능 제품에 대한 소프트웨어 사이버보안 표준, 파트 1: 일반 요구 사항

26. UL 2900-2-1:2017, 네트워크 연결 가능 제품을 위한 소프트웨어 사이버보안, 파트 2-1: 의료 및 웰니스 시스템의 네트워크 연결 가능 컴포넌트에 대한 특정 요구 사항

12.3. 규정 지침 및 초안 지침

27. ANSM(초안): 수명 주기 동안 소프트웨어를 통합하는 의료기기의 사이버보안(2019년 7월)

28. 중국: 의료기기 사이버보안 시판 전 검토 지침(2022년 3월)

29. 유럽 위원회: 유럽 의회 규정(EU) 2017/745 및 2017년 4월 5일 의료기기에 관한 이사회, 개정 지침 2001/83/EC, 규정(EC) 제 178/2002호 및 규정(EC) 제 1223/2009호를 개정하고 이사회 지침 90/385/EEC 및 93/42/EEC(2017년 5월)를 폐지한다.

30. 유럽 위원회: 유럽 의회 규정(EU) 2017/746 및 체외 진단 의료기기에 관한 2017년 4월 5일 이사회 및 지침 98/79/EC 및 위원회 결정 2010/227/EU(2017년 5월)를 폐지한다.

31. FDA(초안): 의료기기의 사이버보안: 품질 시스템 고려 사항 및 콘텐츠 시판 전 제출(2022년 4월) [이 지침은 이 N73 발행 시점의 초안이며 시행을 위한 것이 아니다. 최종 지침으로 대체될 예정이다.]

32. FDA: 상용 소프트웨어(OTS: Off-the-Shelf)가 포함된 네트워크 의료기기의 사이버보안(2005년 1월)

33. FDA: 가정용 의료기기의 설계 고려 사항(2014년 11월)

34. FDA: 의료기기 사이버보안의 시판 후 관리(2016년 12월)

35. 독일: 네트워크 연결 의료기기에 대한 사이버보안 요구 사항(2018년 11월)

36. 독일(BSI) - e헬스 애플리케이션에 대한 보안 요구 사항 기술 지침(BSI TR- 03161)(2020년 4월)

37. 캐나다 보건부: 의료기기 사이버보안에 대한 시판 전 요구 사항

(2019년 6월)

38. 일본: 의료기기의 사이버보안 보장: PFSB/ELD/OMDE 고시 번호 0428-1(2015년 4월)

39. 일본: 의료기기의 사이버보안 보장에 관한 지침: PSEHB/MDED-PSD 고시 제0724-1호(2018년 7월)

40. 의료기기 조정 그룹(MDCG) 2019-16: 의료기기 사이버보안 지침 (2019년 12월)

41. 싱가포르 표준 위원회 기술 참조 67: 의료기기 사이버보안 (2018)

42. TGA: 업계를 위한 의료기기 사이버보안 지침(2019년 7월)

43. TGA: 사용자를 위한 의료기기 사이버보안 정보(2019년 7월)

12.4. 기타 자원 및 참고 문헌

44. CERT® 조정된 취약점 공개 지침 https://resources.sei.cmu.edu/asset_files/SpecialReport/2017_003_001_503340.pdf

45. NIST 사이버보안 프레임워크
https://www.nist.gov/cyberframework

46. NIST의 시큐어 소프트웨어 개발 프레임워크(SSDF: Secure Software Development Framework)
https://csrc.nist.gov/CSRC/media/Publications/white-paper/2019/06/07/mitigating-risk-of-software-vulnerabilities-with-ssdf/draft/documents/ssdf-for-mitigating-risk-of-software-vulns-draft.pdf

47. NIST 특별 간행물 800-12 Rev 1 정보 보안 소개(2017년 6월)
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

48. 의료기기 및 헬스 IT 공동 보안 계획(2019년 1월)
https://healthsectorcouncil.org/wp-content/uploads/2019/01/HSCC-MEDTECH-JSP-v1.pdf

49. MITRE 의료기기 사이버보안 플레이북(2018년 10월)
https://www.mitre.org/publications/technical-papers/medical-device-cybersecurity-regional-incident-preparedness-and

50. MITRE CVSS 헬스케어 루브릭(Rubric)
https://www.mitre.org/publications/technical-papers/rubric-for-app

lying-cvss-to-medical-devices

51. 의료 산업 사이버보안 실무: 위협 관리 및 환자 보호(HICP: Health Industry Cybersecurity Practices)
https://www.phe.gov/preparedness/planning/405d/documents/hicp-main-508.pdf

52. 의료 산업 사이버보안 실무: 레거시 기술 보안 관리 (HIC-MaLTS)
Health-Industry-Cybersecurity-Managing-Legacy-Technology-Security-HIC-MaLTS.pdf(healthsectorcouncil.org)

53. 오픈 웹 애플리케이션 보안 프로젝트(OWASP: Open Web Application Security Project)
https://www.owasp.org/index.php/Main_Page

54. 의료기기 보안을 위한 제조업체 공개 진술서(MDS^2)
https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device Security.aspx

55. 의료기기(MD)에 NIST 프레임워크를 적용하는 ECRI 접근 방식
https://www.ecri.org/components/HDJournal/Pages/Cybersecurity-Risk-Assessment-for-Medical Devices.aspx

56. 미국 국가통신정보국(NTIA) / 상무부(Dept of Commerce), 취약점 공개 태도 및 조치: NTIA 인식 및 채택 그룹의 연구 보고서 https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf